数学名著译丛

数论中未解决的问题

（第二版）

〔加〕R. K. 盖伊 著

张明尧 译

科学出版社

北京

内 容 简 介

本书分6个部分，介绍了数论中大量未解决的问题（个别问题现在已解决了），其中包括：素数，整除性，堆垒数论，不定方程，整数序列及其他问题. 目的是向初次涉及研究工作的人以及有一定工作经历，但缺乏合适的数学问题的人，提供一批容易理解（即便并不容易解决）的问题.

本书可供科研人员，大学数学系师生，数学爱好者阅读.

Translation from the English Language edition:
Unsolved Problems in Number Theory by Richard K. Guy

ISBN 0-387-94289-0

图字：01-2001-0353 号

图书在版编目（CIP）数据

数论中未解决的问题（第二版）/（加）盖伊（Guy，R.K.）著；张明尧译. —北京：科学出版社，2003
（数学名著译丛）
ISBN 7-03-010310-6

Ⅰ.数… Ⅱ.①盖…②张… Ⅲ.数论-数学问题-研究
Ⅳ.O156

中国版本图书馆 CIP 数据核字（2002）第 018818 号

责任编辑：毕 颖/责任校对：钟 洋
责任印制：安春生/封面设计：张 放

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com

丽源印刷厂 印刷
科学出版社发行 各地新华书店经销

*

2003年1月第 一 版 开本：850×1168 1/32
2003年1月第一次印刷 印张：11 3/8
印数：1—3 000 字数：288 000

定价：30.00 元

（如有印装质量问题,我社负责调换〈北燕〉）

中文版前言

中国人和世界上其他文明古国的人民一样，很早就对数学的发展做出了贡献，他们对数学做出的贡献要比世界上多数国家更为久远. 然而东西方的交流一度不是十分通畅. 举例来说，直到最近我们才知道，Catalan 数不仅在 Catalan 之前 100 多年就被 Euler，Fuss 以及 Segner 等人研究过，而且在他们之前就被中国数学家明安图研究过（译者注：明安图（? ～1765)，我国清代数学家、天文学家，字静庵，蒙族人，曾任钦天监监正，主要著作有《割圆密率捷法》四卷等).

中国人对数学的贡献在数论中表现得尤为突出. 在现代中国有华罗庚、闵嗣鹤以及他们的学生，尤其是陈景润、王元和潘承洞，现在又有了第三代数学家. 他们在经典数论的许多问题，诸如 Goldbach 猜想、Gauss 整点问题、Tarry 问题、Waring 问题以及有关素数分布等问题的研究中都取得了重要的成果，并且正在做着重要的贡献.

在这里我要感谢译者张明尧在将我这本激励了众多西方读者的数论问题集介绍给中国读者时所做的工作. 如果书中任何问题有了新的进展，请读者不吝赐教，以便这些新的进展可以写进本书未来的新版之中.

R. K. 盖伊

2002 年 3 月

卡尔加里大学

阿尔伯塔，加拿大

第二版前言

Erdös 回忆起 1912 年在剑桥举行的国际数学家大会上，Landau 曾就素数和提及的在当时的学术条件下无法解决的 4 个问题（见下面的 A1，A5，C1）作过一个讲话. 他说这些问题现在仍然无法解决. 另一方面，自本书第一版问世以来，已有了一些惊人的进展. Fermat 大定理（有个小的漏洞预期可得以弥补）、Mordell 猜想、Carmichael 数的无穷性等一批问题已经获得解决. (Fermat 大定理证明中的漏洞已由 Andrew Wiles 等人完全解决——译者注)

本书永远是落后于时代的，其差距虽然并不总是像在第一版的问题 D1 中一个命题那样有 1700 年之久，但至少在昨天的条目和读者阅读首批上市的新书之间要相差几个月的时间. 为使读者与本书第一版容易进行比较，每节的编号保持不变. 大部或全部获得解决的问题有 B47，D2，D6，D8，D16，D26，D27，D28，E15，F15，F17 及 F28. 在某些情形附加了一些有关的开放问题；而在另一些情形，涉及到的一些没有解决的问题不是作为问题，而是作为练习放了进来.

现将作者的两个特别喜欢使用的符号说明如下：其一是用 & 表示合作的工作，以消除任何可能的含混不清之处. 例如"……得自 Gauss 的工作以及 Erdös 和（&）Guy 的工作"；其二是从匈牙利人那儿借用的符号¿……?，它表示一个猜测或假想的命题. 一本初等微积分教材的作者，他有良好的意图却未得到好的建议. 如果他能在书中用此符号，当可避免某些精神上的痛楚. 有一个学生在求乘积函数的导数时发生了困难，在我感到失望之时，我想到要求看一看那个学生的教科书. 我看到他在书上用醒目的记号标出一个公式：乘积的导数等于导数的乘积. 可是

他却没有注意到书上说的是“为什么……不是正确的答案?”

以前提到的《几何中未解决的问题》一书现已出版，而且是作为重印本或作为第二版发行.

由本书可以清楚地看到，有多少人接受了我的邀请，利用它来交换有关问题的信息；而我又是如何从与读者的通信中获益匪浅的. 尽管我已经将致谢的名单大大扩大了，但这份名单仍不完全. 不过我至少应该感谢 Harvey Abbott，Arthur Baragar，Paul Bateman，T. G. Berry，Andrew Bremner，John Brillhart，R. H. Buchholz，Duncan Buell，Joe Buhler，Mitchell Dickerman，Hugh Edgar，Paul Erdös，Steven Finch，Aviezri Fraenkel，David Gale，Sol Golomb，Ron Graham，Sid Graham，Andrew Granville，Heiko Harborth，Roger Heath-Brown，Martin Helm，Gerd Hofmeister，Wilfrid Keller，Arnfried Kemnitz，Jeffrey Lagarias，Jean Lagrange，John Leech，Dick Lehmer，Emma Lehmer，Hendrik Lenstra，Hugh Montgomery，Peter Montgomery，Shigeru Nakamura，Richard Nowakowski，Andrew Odlyzko，Richard Pinch，Carl Pomerance，Aaron Potler，Herman te Riele，Raphael Robinson，Øystein Rødseth，K. R. S. Sastry，Andrzej Schinzel，Reese Scott，John Selfridge，Ernst Selmer，Jeffrey Shallit，Neil Sloane，Stephane Vandemergel，Benne de Weger，Hugh Williams，Jeff Young 和 Don Zagier. 没有 John Leech 完美的校对，没有他广博的文献知识以及明晰的数学思想和创见，本书将会大为逊色.

作者还要感谢 Andy Guy 为本书创建的电子体系，它使得作者和出版社两方面的工作都轻松了许多. 我们还要感谢加拿大国立科学和工程研究理事会对本书和作者的许多其他项目始终如一的支持.

R. K. 盖伊

1994. 1. 8 于卡尔加里

第一版前言

在许多外行人看来，数学家好像就是解题之人，也就是俗话说的“解算术难题的人”. 即便在数学界内部，数学家们也把自己分成理论研究者和问题求解者两类人. 数学能保持其生命力，比上述两类人的工作更为重要的是依赖于来自数学本身以及来自日益增多的应用领域的一系列问题. 数学常受惠于提出问题者比受惠于回答问题者要更多. 求解一个问题或许会抑制人们对该领域的兴趣. 而“Fermat 大定理”正因为还不是一个定理，它产生了大量“好的”数学——至于数学的好坏，是由它的美、深度及可应用性来加以判别的.

提出好的未解决问题是一门艰难的艺术. 在平庸无聊的问题和几乎无望求解的问题之间求得平衡是困难而微妙的. 有许多易于表述的问题，专家告诉我们，这些问题到下一代也不太可能获得解决. 即使我们不能活着看到 Riemann 猜想、Goldbach 猜想、孪生素数猜想、Mersenne 素数猜想或者奇完全数猜想的解决，然而我们却看到了四色猜想的解决. 从另一方面来说，“未解决的”问题未必就是根本不可解的，或许可能比我们一开始所想的要容易得多.

在匈牙利数学家 P. Erdös 所做出的许多贡献中，并非最不起眼的是他源源不断提出来的一系列出色的问题. 好像这些问题还不够刺激似的，他还对许多问题的第一个解决者予以悬赏奖励，同时对问题的难度给出他自己的估计. 为此他已付出了许多钱，奖金从 1 美元到 1000 美元不等.

本书的目的之一是向初次涉及研究工作的人以及那些虽然更为成熟、但缺乏合适的数学问题刺激的人提供一批容易理解（即便并不容易解决）的问题. 他们可以在不同的深度上考虑这些问

题，有时能获得部分进展，从而逐渐赢得兴趣、信心和恒心，这些都是研究工作获得成功的要素.

本书还有更为广泛的目标. 对那些水平高低各不相同的学习数学的学生和数学教师来说，虽然他们没有能力做研究工作，或许对此也并无希冀或雄心，然而重要的是有大批他们能够理解的未解决的问题，其中有些问题会在他们的一生中得到解决. 有许多业余数学爱好者被吸引过来，有许多成功的研究工作者一开始就是通过对 Euclid 几何、数论中的问题（最近是对组合和图论中的问题）加以研究而赢得信心的. 在这些领域中他们有可能不需要在理论上有很深的预备知识就看得懂问题，甚至能用式子表达问题并得到初步的结果.

本书的思想可追溯到大约 20 年前，那时我被流传的由已故的 Leo Moser 及其合作者 Hallard Croft 所写的问题册以及 Erdös 的文章深深吸引. Croft 同意让我帮助他把他的问题册扩大写成一本书，而 Erdös 则不断地鼓励、督促我们. 过了一些时候，数论这一章已经膨胀成了一部系列丛书中的一卷，这一系列丛书还将包括几何卷、凸性和分析卷，它们由 Hallard Croft 撰写，另外还有一卷关于组合、图论和博弈的书，由本书作者撰写.

为了节省读者翻阅的时间，参考文献（有时是范围广泛的文献资料）放在每一个问题的末尾，或放在一组问题的综述中.

有许多人看过本书的部分手稿，与作者通过信并给出过有益的评论，其中有一些是已去世的友人；Harold Davenport, Hans Heibronn, Louis Mordell, Leo Moser, Theodor Motzkin, Alfred Rényi 和 Paul Turán. 此外还有 H. L. Abbott, J. W. S. Cassels, J. H. Conway, P. Erdös, Martin Gardner, R. L. Graham, H. Halberstam, D. H. Lehmer, Emma Lehmer, A. M. Odlyzko, Carl Pomerance, A. Schinzel, J. L. Selfridge, N. J. A. Sloane, E. G. Straus, H. P. F. Swinnerton-Dyer 和 Hugh Williams. 由加拿大国立（科学和工程）研究理事会提供的资助，使我们有条件与上述各位及其他许多人取得联系. 在本书最后定稿的过程中，

卡尔加里（Calgary）大学授予的 Killam Resident 研究基金给了我特别有用的帮助. 书稿的打印工作是由 Karen Mcdermid，Betty Teare 和 Louise Guy 完成的，他们还帮忙做了校对. 此外，纽约的斯普林格出版分社的全体职员诚挚有礼、称职能干，对我们助益良多.

尽管有这些帮助，书中难免会有许多错误，对此我承担全部责任. 无论如何，只要本书服务其目的，那么它从问世的那一刻起就已经过时了，而且一旦写作开始，它就已经在变得过时. 有鉴于此，我乐于听到来自读者的声音，因为一定会有许多我所不知道的解、文献以及问题. 我希望各位能借交流有关的信息而获益. 有一些出色的研究工作者通过自己重新发现这些结果而在事业上兴旺发达起来，但我们中的许多人在了解到自己的发现已早为他人所为后变得沮丧而失望.

R. K. 盖伊

1981. 8. 13 于卡尔加里

目　　录

符　号

A.P.	算术级数 $a, a+d, \cdots, a+kd, \cdots$	A6,E10,E33
$a_1 \equiv a_2 (\bmod b)$	a_1 同余于 a_2(modulo d)，即 $a_1 - a_2$ 被 b 整除	A3,A4,A12,A15,B2,B4,B7,…
$A(x)$	一个数列中不超过 x 的元素个数,例如不超过 x 的亲和数的个数	B4,E1,E2,E4
c	正常数	A1, A3, A8, A12, B4,B11,…
d_n	相邻素数差 $p_{n+1} - p_n$	A8,A10,A11
$d(n)$	n 的(正)因子个数,即 $\sigma_0(n)$	B, B2, B8, B12, B18, …
$d \mid n$	d 整除 n，n 是 d 的倍数，存在一个整数 q 使 $dq = n$	B,B17,B32,B37,B44,C20,D2,E16
$d \nmid n$	d 不整除 n	B, B2, B25, E14, E16,…
e	自然对数的底，2.718281828459045…	A8,B22,B39,D12,…
E_n	Euler 数，sec x 的级数展开式中的系数	B45
exp{ }	指数函数	A12, A19, B4, B36,B39,…

F_n	Fermat 数,$2^{2^n}+1$	A3,A12
$f(x)\sim g(x)$	$\frac{f(x)}{g(x)}\to 1(x\to\infty)(f,g>0)$	A1, A3, A8, B33, B41,C1,C17, D7, E2,E30,F26
$f(x)=o(g(x))$	$\frac{f(x)}{g(x)}\to 0(x\to\infty)(g>0)$	A1,A18,A19,B4, C6,C9,C11,C16, C20,D4,D11,E2, E14,F1
$f(x)=O(g(x))$	(即 $f(x)\ll g(x)$) 存在一个 c 使对所有充分大的 x 有 $\lvert f(x)\rvert<cg(x)(g(x)>0)$	A19,B37,C8,C9, C10,C12,C16, D4, D12, E4, E8, E20, E30, F1, F2, F16 A4, B4, B18, B32, B40,C9,C14, D11,E28,F4
$f(x)=\Omega(g(x))$	存在一个 $c>0$ 使得有任意大的 x 存在使 $\lvert f(x)\rvert\geqslant cg(x)(g(x)>0)$	D12,E25
$f(x)\asymp g(x)$	(即 $f(x)=\Theta(g(x))$) 存在 c_1,c_2 使对所有充分大的 x 有 $c_1g(x)\leqslant f(x)\leqslant c_2g(x)(g(x)>0)$	B18 E20
i	-1 的平方根,$i^2=-1$	A16
$\ln x$	x 的自然对数	A1, A2, A3, A5, A8,A12,…

(m,n)	m 和 n 的最大公约数 g. c. d., m 和 n 的最高公因子 h. c. f.	B3,B4,B5,B11,D2
$[m,n]$	m 和 n 的最大公约数 l. c. m.,	B35,E2,F14
	也用来代表相连整数 $m, m+1, \cdots, n$ 的集合	B24,B26,B32,C12,C16
$m \perp n$	m 和 n 互素 $(m,n)=1$	A,A4,B3,B4,B5,B11,D2
M_n	Mersenne 素数 2^n-1	A3,B11,B38
$n!$	n 的阶乘;$1\times2\times3\times\cdots\times n$	A2,B12,B14,B22,B23,B43,…
$!n$	$0!+1!+2!+\cdots+(n-1)!$	B44
$\binom{n}{k}$	从 n 个元素中任取 k 个元素的取法数,二项系数 $\frac{n!}{k!(n-k)!}$	B31,B33,C10,D3
$\left(\frac{p}{q}\right)$	Legendre(或 Jacobi)符号	见 F5(A1,A12,F7)
$p^a \parallel n$	p^a 整除 n,但 p^{a+1} 不整除 n	B,B8,B37,F16
p_n	第 n 个素数,其中 $p_1=2$, $p_2=3$, $p_3=5$,…	A2,A5,A14,A17,E30
$p(n)$	n 的最大素因子	B30,B46
Q	有理数域	D2,F7
$r_k(n)$	不超过的数中必定包含一个有个项的算术级数的数的最少个数	见 E10
$s(n)$	n 的除去 n 以外的所有正因	B,B1,B2,B8,B10,…

	子之和,$\sigma(n)-n$	
$s^k(n)$	$s(n)$的第 k 次迭代	B,B6,B7
$s^*(n)$	如果 $d\mid n$ 且$\left(d,\frac{n}{d}\right)=1$,则称 d 为 n 的一个单因子. $s^*(n)$表示 n 的除去 n 以外的所有单因子的和	B8
$S\cup T$	集合 S 与 T 的并	E7
$W(k,l)$	van der Waerden 数	见 E10
$\lfloor x\rfloor$	x 的底,即不大于 x 的最大整数	A1, A5, C7, C12, C15, …
$\lceil x\rceil$	x 的顶,即不小于 x 的最小整数	B24
$\mathbb{Z}$	整数…, −2, −1,0,1,2,…	F14
$\mathbb{Z}_n$	整数环 0, 1, 2, …, $n-1$ (mod$n$)	E8
γ	Euler 常数, 0.577215664901532…	A8
ε	任意小的正常数	A8, A18, A19, B4, B11, …
ζ_p	p 次单位根	D2
$\zeta(s)$	Riemannζ 函数; $\sum_{n=1}^{\infty}\frac{1}{n^s}$	D2
π	圆的周长与直径之比; 3.141592653589793…	F1,F17
$\pi(x)$	不超过 x 的素数个数	A17,E4
$\pi(x;a,b)$	不超过 x 且模b 与a 同余的素数个数	A4
$\prod$	乘积	A1,A2,A3,A8,A15, …

$\sigma(n)$	n 的所有因子之和；即 $\sigma_1(n)$	B,B2,B5,B8,B9, …
$\sigma_k(n)$	n 的所有因子的 k 次幂之和	B,B12,B13,B14
$\sigma^k(n)$	$\sigma(n)$的第 k 次迭代	B9
$\sigma^*(n)$	n 的所有单因子之和	B8
$\sum$	求和	A5, A8, A12, B2, B14, …
$\varphi(n)$	Eulerφ 函数；不超过 n 且与 n 互素的正整数的个数	B8, B11, B36, B38, B39, …
$\varphi^k(n)$	$\varphi(n)$的第 n 次迭代	B41
ω	1 的三次复根，即 $\omega^3=1,\omega\neq1,\omega^2+\omega+1=0$	A16
$\omega(n)$	n 的不同素因子的个数	B2,B8,B37
$\Omega(n)$	n 的所有素因子的个数（按重数计算）	B8
¿ . . . ?	猜想或假设的命题	A1, A9, B37, C6, E10,E28,F2,F18

引　言

长期以来,无论对数学业余爱好者还是职业数学工作者来说,数论比其他任何数学分支都更有吸引力. 以致现在它的许多部分都有相当的技术性困难. 然而,仍有比以前更多的未解决的问题,其中许多问题虽然不太可能在下一代手中得到解决,这仍无法阻止人们去尝试. 未解决的问题是如此之多,连整整一卷书也装不下它们. 现在的这本书只不过是作者本人选出的一些范例.

数论中问题的一些可靠的出处曾列在本书第一版的引言中,其中的一部分重新列在下面,同时还列出了一些较新的资料.

Paul Erdös, Problems and results in combinatorial number theory III, *Springer Lecture Notes in Math.*, **626** (1977) 43~72; *MR* **57** #12442.

Paul Erdös, A survey of problems in combinatorial number theory, in *Combinatorial Mathematics, Optimal Designs and their Applications* (Proc. Symp. Colo. State Univ. 1978) *Ann. Discrete Math.*, **6**(1980) 89—115.

Paul Erdös & R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographies de l'Enseignement Math. No. 28, Geneva, 1980.

Paul Erdös, & András Sárközy, Some solved and unsolved problems in combinatorial number theory, *Math. Slovaca*, **28** (1978) 407~421; *MR* **80I**:10001.

Paul Erdös, Problems and results in number theory, in Halberstam & Hooley (eds) Recent Progress in Analytic Number Theory, Vol. 1, Academic Press, 1981, 1~13.

H. Fast & S. Swierczkowski, *The New Scottish Book*, Wroclaw,

1946～1958.

Heini Halberstam, Some unsolved problems in higher arithmetic, in Ronald Duncan & Miranda Weston-Smith (eds.) *The Encyclopedia of Ignorance*, Pergamon, Oxford & New York, 1977, 191～203.

Victor Klee & Stan Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Math. Assoc. Of Amer. Dolciani Math. Expositions, **11**(1991).

Proceedings of Number Theory Conference, Univ. of Colorado, Boulder, 1963.

Report of Institute in the Theory of Numbers, Univ. of Colorado, Boulder, 1959.

Joe Roberts, *Lure of the Integers*, Math. Assoc. of America, Spectrum Series, 1992.

Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 2nd ed. 1978; *MR* **80e**:10003.

W. Sierpiński, *A selection of Problems in the Theory of Numbers*, Pergamon, 1964.

Robert D. Silverman, A perspective on computational number theory, in Computers and Mathematics, *Notices Amer. Math. Soc.*, 38(1991) 562～568.

S. Ulam, *A Collection of Mathematical Problems*, Interscience, New York, 1960.

在本书中,"数"表示自然数,即

$$0,1,2,\cdots$$

而 c 表示绝对正常数,每次出现时不一定都取同样的值. 我们利用 K. E. Iverson 的现已为大家熟悉的符号"底"($\lfloor\ \rfloor$)和"顶"($\lceil\ \rceil$)来分别表示"不大于……的最大整数"和"不小于……的最小整数". 一个不大熟悉的符号是用"$m\perp n$"表示"m 与 n 互素",即"$\gcd(m,n)=1$".

本书根据我个人的想法划分成6个部分：

A. 素数

B. 整除性

C. 堆垒数论

D. 不定方程

E. 整数序列

F. 不在上述各章中的其他问题.

A. 素　数

可以把正整数分成三类:

单位(unit)　1

素数(prime) 2,3,5,7,11,13,17,19,23,29,31,37,…

合数(composite) 4,6,8,9,10,12,14,15,16,….

一个大于 1 的数是素数,如果它仅有的正因子是 1 和它自己;反之则称它为合数. 至少从 Euclid 开始,数学家们就对素数感兴趣了. Euclid 曾经证明了素数有无穷多个.

用 p_n 表示第 n 个素数,例如 $p_1=2$, $p_2=3$, $p_{99}=523$;用 $\pi(x)$表示不大于 x 的素数个数,例如 $\pi(2)=1$, $\pi\left(3\frac{1}{2}\right)=2$, $\pi(1000)=168$, $\pi(4\times10^{16})=1075292778753150$. 用$(m,n)$表示 m 和 n 的最大公因子(gcd),例如$(36,66)=6$, $(14,15)=1$, $(1001,1078)=77$. 如果$(m,n)=1$,就说 m 和 n 互素(coprime),记为 $m\perp n$,例如 $182\perp165$.

Dirichlet 定理告诉我们:只要 $a\perp b$,在任何算术级数(arithmetic progression)

$$a, a+b, a+2b, a+3b, \cdots$$

中必有无穷多个素数. 下文对有关素数的问题和进一步的参考资料给出了综述:

A. Schinzel & W. Sierpiński, Sur certains hypothèses concernant les nombres premiers, *Acta Arith*. , 4(1958) 185-208; erratum5(1959) 259; *MR* 21#4936;又见 7(1961)1-8.

问题 D27 中的表 7 可以用作为小于 1000 的素数表;表中写有数字 1,3,5,7 对应的数都是素数,而 1,3,5,7 指的是该素数模 8 所在的剩余类(见 A4).

多年来,确定一个大数是素数还是合数,而在它为合数时确定它的因子这样一个一般性的问题一直吸引着数论学者. 随着高速计算机的出现,问题取得了相当大的进展. 近来还由于它对密码分析学的应用,对这一问题的研究又提供了新的动力. 其他一些文献放在问题 A3 之后及本书第一版中.

参考文献

William Adams & Daniel Shanks, Strong primality tests that are not sufficient, *Math. Comput.*, **39**(1982) 255–300.

Richard K. Guy, How to factor a number, *Congressus Numerantium XVI*, Proc. 5th Manitoba Conf. Numer. Math., Winnipeg, 1975, 49–89; *MR* **53** #7924.

Wilfrid Keller, Woher kommen die größten derzeit bekannten Primzahlen? *Mitt. Math. Ges. Hamburg*, **12**(1991) 211–229; *MR* **92j**:11006.

Arjen K. Lenstra & Mark S. Manasse, Factoring by electronic mail, in Advances in Cryptology—EUROCRYPT'89, *Springer Lect. Notes in Comput. Sci.*, **434**(1990) 355–371; *MR* **91i**:11182.

Hendrik W. Lenstra, Factoring integers with elliptic curves, *Ann. of Math.*(2), **126**(1987) 649–673; *MR* **89g**:11125.

Hendrik W. Lenstra & Carl Pomerance, A rigorous time bound for factoring integers, *J. Amer. Math. Soc.*, **5**(1992) 483–916; *MR* **92m**:11145.

G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci.*, **13**(1976) 300–317; *MR* **58** #470ab.

Peter Lawrence Montgomery, An FFT extension of the elliptic curve method of factorization, PhD dissertation, UCLA, 1992.

J. M. Pollard, Theorems on factoring and primality testing, *Proc. Cambridge Philos. Soc.*, **76**(1974) 521–528; *MR* **50** #6992.

J. M. Pollard, A Monte Carlo method for factorization, *BIT*, **15**(1975) 331–334; *MR* **52** #13611.

Carl Pomerance, Recent developments in primality testing, *Math. Intelligencer*, **3**(1980/81) 97–105.

Carl Pomerance, Notes on Primality Testing and Factoring, *MAA Notes* **4**(1984) Math. Assoc. of America, Washington DC.

Carl Pomerance (editor), Cryptology and Computational Number Theory, *Proc. Symp. Appl. Math.*, **42** Amer. Math. Soc., Providence, 1990; *MR* **91k**: 11113.

Paulo Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, New York, 1988.

Paulo Ribenboim, *The Little Book of Big Primes*, Springer-Verlag, New York, 1991.

Hans Riesel, Wie schnell kann man Zahlen in Faktoren zerlegen? *Mitt. Math. Ges. Hamburg*, **12**(1991) 253–260.

R. Rivest, A. Shamir & L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications A.C.M.*, Feb. 1978.

R. Solovay & V. Strassen, A fast Monte-Carlo test for primality, *SIAM J. Comput.*, **6**(1977) 84-85; erratum **7**(1978) 118; *MR* **57** #5885.

Jonathan Sorenson, Counting the integers cyclotomic methods can factor, *Comput. Sci. Tech. Report*, **919**, Univ. of Wisconsin, Madison, March 1990.

H. C. Williams & J. S. Judd, Some algorithms for prime testing using generalized Lehmer functions, *Math. Comput.*, **30**(1976) 867-886.

A1. 取素数值的二次函数

有无穷多个形如 a^2+1 的素数吗？可能如此．事实上 Hardy 和 Littlewood(在他们的猜想 E 中)曾猜想：小于 n 的这种素数的个数 $P(n)$ 渐近地等于 $c\sqrt{n}/\ln n$，

$$¿\quad P(n)\sim c\sqrt{n}/\ln n\quad ?$$

即 $P(n)$ 与 $\sqrt{n}/\ln n$ 的比值当 $n\to\infty$ 时趋向于 c．常数 c 等于

$$c=\prod\left\{1-\frac{\left(\frac{-1}{p}\right)}{p-1}\right\}=\prod\left\{1-\frac{(-1)^{(p-1)/2}}{p-1}\right\}\approx 1.3727,$$

其中 $\left(\frac{-1}{p}\right)$ 是 Legendre 符号(见 F5)，该乘积取过所有奇素数．对于用更为一般的二次多项式表示的素数之个数这一问题，他们做出了类似的猜想，仅仅常数 c 的值有所不同．但是我们尚不知道有哪一个高于一次的多项式已被证明能取到无穷多个素数值．是否对每个 $b>0$，都有一个形如 a^2+b 的素数呢？Sierpiński 曾经证明了：对每个 k，存在一个 b，使得有多于 k 个形如 a^2+b 的素数．

Iwaniec 证明了存在无穷多个 n，使 n^2+1 是至多两个素数之积．他的结果可以推广到其他二次不可约多项式上去．

如果 $P(n)$ 表示 n 的最大素因子，Maurice Mignotte 证明了当 $a\geqslant 240$ 时有 $P(a^2+1)\geqslant 17$．注意到有 $239^2+1=2\times 13^4$(这是数 239 的又一个性质)．50 年来人们就已经知道 $P(a^2+1)\to\infty\ (a\to\infty)$．

Ulam 和其他人注意到，当数列写成"方形螺线"时，似乎在与

某种“富含素数”的二次多项式对应的对角线上更容易出现素数. 例如,图 1 的主对角线就对应 Euler 著名的公式 n^2+n+41.

421	420	**419**	418	417	416	415	414	413	412	411	410	**409**	408	407	406	405	404	403	402
422	**347**	346	345	344	343	342	341	340	339	338	**337**	336	335	334	333	332	**331**	330	**401**
423	348	**281**	280	279	278	**277**	276	275	274	273	272	**271**	270	**269**	268	267	266	329	400
424	**349**	282	**223**	222	221	220	219	218	217	216	215	214	213	212	**211**	210	265	328	399
425	350	**283**	224	**173**	172	171	170	169	168	**167**	166	165	164	**163**	162	209	264	327	398
426	351	284	225	174	**131**	130	129	128	**127**	126	125	124	123	122	161	208	**263**	326	**397**
427	352	285	226	175	132	**97**	96	95	94	93	92	91	90	121	160	207	262	325	396
428	**353**	286	**227**	176	133	98	**71**	70	69	68	**67**	66	**89**	120	159	206	261	324	395
429	354	287	228	177	134	99	72	**53**	52	51	50	65	88	119	158	205	260	323	394
430	355	288	**229**	178	135	100	**73**	54	**43**	42	49	64	87	118	**157**	204	259	322	393
431	356	289	230	**179**	136	**101**	74	55	44	**41**	48	63	86	117	156	203	258	321	392
432	357	290	231	180	**137**	102	75	56	45	46	**47**	62	85	116	155	202	**257**	320	391
433	358	291	232	**181**	138	**103**	76	57	58	**59**	60	**61**	84	115	154	201	256	319	390
434	**359**	292	**233**	182	**139**	104	77	78	**79**	80	81	82	**83**	114	153	200	255	318	**389**
435	360	**293**	234	183	140	105	106	**107**	108	**109**	110	111	112	**113**	152	**199**	254	**317**	388
436	361	294	235	184	141	142	143	144	145	146	147	148	**149**	150	**151**	198	253	616	387
437	362	295	236	185	186	187	188	189	190	**191**	192	**193**	194	195	196	**197**	252	315	386
438	363	296	237	238	**239**	240	**241**	242	243	244	245	246	247	248	249	250	**251**	314	385
439	364	297	298	299	300	301	302	303	304	305	306	**307**	308	309	310	**311**	312	**313**	384
440	365	366	**367**	368	369	370	371	372	**373**	374	375	376	377	378	**379**	380	381	382	**383**

图 1　素数(用黑体表示者)构成对角图案

有一些次数大于 1 的(多项式)表示素数的结果,它们起源于 Pyateckii-Šapiro. 他证明了:如果 $1\leqslant c\leqslant\frac{12}{11}$,那么在范围 $1<n<x$ 中形如$\lfloor n^c\rfloor$的素数个数等于

$$(1+o(1))x/(1+c)\ln x.$$

其中的数$\frac{12}{11}$先后被 Kolesnik, Graham 和 Leitmann, Heath-Brown, Kolesnik 以及刘弘泉(Liu Hong-Quan)和 Rivat 相继改进为$\frac{10}{9}$, $\frac{69}{62}$, $\frac{755}{662}$, $\frac{39}{34}$和$\frac{15}{13}$.

参考文献

Gilbert W. Fung & Hugh Cowie Williams, Quadratic polynomials which have a high density of prime values, *Math. Comput.*, **55**(1990) 345–353; *MR* **90j**:11090.

Martin Gardner, The remarkable lore of prime numbers, *Scientific Amer.*, **210**

#3 (Mar. 1964) 120–128.

G. H. Hardy & J. E. Littlewood, Some problems of 'partitio numerorum' III: on the expression of a number as a sum of primes, *Acta Math.*, **44**(1922) 1–70.

D. R. Heath-Brown, The Pyateckii-Šapiro prime number theorem, *J. Number Theory*, **16**(1983) 242–266.

D. R. Heath-Brown, Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression, Proc. London Math. Soc.(3) **64**(1992) 265–338.

Henryk Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.*, **47**(1978) 171–188; *MR* **58** #5553.

G. A. Kolesnik, The distribution of primes in sequences of the form $[n^c]$, *Mat. Zametki*(2), **2**(1972) 117–128.

G. A. Kolesnik, Primes of the form $[n^c]$, *Pacific J. Math.*(2), **118**(1985) 437–447.

D. Leitmann, Abschätzung trigonometrischer Summen, *J. reine angew. Math.*, **317**(1980) 209–219.

D. Leitmann, Durchschnitte von Pjateckij-Shapiro-Folgen, *Monatsh. Math.*, **94**(1982) 33–44.

H. Q. Liu & J. Rivat, On the Pyateckii-Šapiro prime number theorem, *Bull. London Math. Soc.*, **24**(1992) 143–147.

Maurice Mignotte, $P(x^2+1) \geq 17$ si $x \geq 240$, *C. R. Acad. Sci. Paris Sér. I Math.*, **301**(1985) 661–664; *MR* **87a**:11026.

Carl Pomerance, A note on the least prime in an arithmetic progression, *J. Number Theory*, **12**(1980) 218–223.

I. I. Pyateckii-Šapiro, On the distribution of primes in sequences of the form $[f(n)]$ (Russian), *Mat. Sbornik N.S.*, **33**(1953) 559–566; *MR* **15**, 507.

Daniel Shanks, On the conjecture of Hardy and Littlewood concerning the number of primes of the form n^2+a, *Math. Comput.*, **14**(1960) 321–332.

W. Sierpiński, Les binômes x^2+n et les nombres premiers, *Bull. Soc. Roy. Sci. Liège*, **33**(1964) 259–260.

E. R. Sirota, Distribution of primes of the form $p=[n^c]=[t^d]$ in arithmetic progressions (Russian), *Zap. Nauchn. Semin. Leningrad Otdel. Mat. Inst. Steklova*, **121**(1983) 94–102; *Zbl.* **524**.10038.

A2. 与阶乘有关的素数

是否有无穷多个形如 $n!\pm 1$ 的素数？或无穷多个形如

$$X_k = 1 + \prod_{i=1}^{k} p_i$$

的素数？或无穷多个形如 $X_k - 2$ 的素数？Buhler, Crandall 和 Penk 证明了：当 $n = 1,2,3,11,27,37,41,73,77,116,154,320,340,399,427$ 时 $n!+1$ 是素数；对 $n<546$，仅当 $n=3,4,6,7,12,$

14,30,32,33,38,94,166,324,379,469 时 $n!-1$ 才是素数;对 $p_k<3088$,仅当 $p_k=2,3,5,7,11,31,379,1019,1021,2657$ 时 X_k 才是素数;当 $p_k=3,5,11,13,41,89,317,337,991,1873,2053$ 时 X_k-2 是素数;而当 $p_k=2377$ 时 X_k-2 有可能是素数(尚未对此作出检验). Harvey Dubner 发现 $872!+1$ 和 $1477!+1$ 是素数,而对 $p_k=3229,4547,4787$, X_k 是素数. 又对 $p_k=11549$ 和 13649, X_k 仍为素数.

令 q_k 表示大于 X_k 的最小素数. R. F. Fortune 曾猜想,对所有 k, q_k-X_k+1,都是素数(这样的素数称为吉祥素数,见下文——译者注). 显然,它不能被前 k 个素数整除. Selfridge 注意到:这一猜想的正确性可以从 Schinzel 关于 Cramér 猜想的一种表述推导出来. Cramér 猜想是说,对 $x>8$,在 x 和 $x+(\ln x)^2$ 之间总有一个素数. 基于如下的假设:所涉及的很大的可能是素数的数皆为真正的素数,Stan Wagon 计算出了前 100 个吉祥素数:

3	5	7	13	23	17	19	23	37	61	67	61	71	47	107	59	61	109	89	103
79	151	197	101	103	233	223	127	223	191	163	229	643	239	157	167	439	239	199	191
199	383	233	751	313	773	607	313	383	293	443	331	283	277	271	401	307	331	379	491
331	311	397	331	353	419	421	883	547	1381	457	457	373	421	409	1061	523	499	619	727
457	509	439	911	461	823	613	617	1021	523	941	653	601	877	607	631	733	757	877	641

这一问题的答案也许是肯定的,但是在可以看得见的未来,无论是用计算机还是解析工具,都不大可能解决这些猜想. Schinzel 猜想归因于 Cramér,而 Cramér 猜测有(见 A8 的参考文献)

$$¿\quad \limsup_{n\to\infty}\frac{p_{n+1}-p_n}{(\ln p_n)^2}=1\quad ?$$

Schinzel 注意到:即使对充分大的 x,这个结果也并不能蕴含 x 与 $x+(\ln x)^2$ 之间必有素数存在. 更有希望成立但仍难以证明的是下述的 Erdös 和 Stewart 的猜想:使得

$$n!+1=p_k^a p_{k+1}^b,\quad p_{k-1}\leqslant n<p_k$$

成立的仅有的情形是 $1!+1=2$, $2!+1=3$, $3!+1=7$, $4!+1$

$=5^2$,5! $+1=11^2$ 吗(注意在这五种情形有$(a,b)=(1,0)$,(1,0),(0,1),(2,0)和(0,2))?

Erdös 又问道:是否存在无穷多个素数 p,使对满足 $1\leqslant k! < p$ 的每个 k, $p-k!$ 皆为合数? 例如 $p=101$ 和 $p=211$. 他认为也许求解下列问题会更容易一些:存在无穷多个整数 $n(l! < n \leqslant (l+1)!)$,它们的素因子均大于 l,且所有的数 $n-k!$ $(1\leqslant k\leqslant l)$皆为合数.

参考文献

I. O. Angell & H. J. Godwin, Some factorizations of $10^n \pm 1$, *Math. Comput.*, **28**(1974) 307–308.

Alan Borning, Some results for $k!\pm 1$ and $2\cdot 3\cdot 5\cdots p\pm 1$, *Math. Comput.*, **26**(1972) 567–570.

J. P. Buhler, R. E. Crandall & M. A. Penk, Primes of the form $n! \pm 1$ and $2\cdot 3\cdot 5\cdots p\pm 1$, *Math. Comput.*, **38**(1982) 639–643; corrigendum, Wilfrid Keller, **40**(1983) 727; *MR* **83c**:10006, **85b**:11119.

Harvey Dubner, Factorial and primorial primes, *J. Recreational Math.*, **19** (1987) 197–203.

Martin Gardner, Mathematical Games, *Sci. Amer.*, **243**#6(Dec. 1980) 18–28.

Solomon W. Golomb, The evidence for Fortune's conjecture, *Math. Mag.*, **54**(1981) 209–210.

S. Kravitz & D. E. Penney, An extension of Trigg's table, *Math. Mag.*, **48**(1975) 92–96.

Mark Templer, On the primality of $k!+1$ and $2*3*5*\cdots*p+1$, *Math. Comput.*, **34**(1980) 303–304.

A3. Mersenne 素数,循环整数,Fermat 数,形如 $k\cdot 2^n+2$ 的素数

特殊形状的素数有永恒的兴趣,特别是 **Mersenne 素数** (Mersenne prime)2^p-1. 这里 p 必须是素数,但这并不是使 2^p-1 为素数的充分条件! 例如 $2^{11}-1=2047=23\cdot 89$. 它们与完全数有关(见 B1).

强有力的 Lucas-Lehmer 判别法以及不断升级换代的计算机和使用计算机的更加成熟的技术,使形如 2^p-1 的素数表不断扩大:

2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,2203

2281,3217,4253,4423,9689,9941,11213,19937,21701,

23209,44497,86243,110503,132049,216091,756839,859433,…

Mersenne 素数的个数无疑是无限的,但其证明却毫无希望地超出了我们的能力. 设 $M(x)$表示满足 $p\leqslant x$ 且使 2^p-1 为素数的素数 p 的个数. 试对 $M(x)$给出令人信服的探索讨论. Gillies 曾设想有 $M(x)\sim c\ln x$. H. W. Lenstra, Pomerance 和 Wagstaff 都相信这是对的,实际上他们猜想有

$$¿\quad M(x)\sim e^{\gamma}\log x \quad ?$$

这里的 log 以 2 为底.

已知最大的素数通常是 Mersenne 素数,但有一个时期最大素数的记录是

$$391581\cdot 2^{216193}-1,$$

它是在 1992 年 3 月晚些时候由 J. Brown, L. C. Noll, B. Parady, G. Smith, J. Smith 和 S. Zarantonello 等人发现的. 这一记录被上述 Mersenne 素数表中倒数第二个数所打破,该数是由 Slowinski 和 Gage 发现的.

D. H. Lehmer 令 $S_1=4, S_{k+1}=S_k^2-2$. 若 2^p-1 是一个 Mersenne 素数,他注意到有 $S_{p-2}\equiv 2^{(p+1)/2}$或 $-2^{(p+1)/2}(\bmod 2^p-1)$. 问题是哪一个同余式为真?

Selfridge 猜想,若 n 是一个形如 $2^k\pm1$ 或 $2^{2k}\pm3$ 的素数,则 2^n-1 和$(2^n+1)/3$ 或者同为素数,或者同为合数. 此外,若两数同为素数,则 n 必为所给形状之一. 这是否就是所谓"强小数法则"的一个例子呢? Dickson 在其所著数论史(*Histry of the Theory of Numbers*)第一卷 p. 28 上说道:

> 在给 Tannery 的一封信中(*l'Intermédiaire des math.* , 2(1895) 317)Lucas 说,Mersenne(1644,1647)给出 2^p-1 为素数的一个充分必要条件是:p 是形如 $2^{2n}+1$,$2^{2n}\pm3$ 或 $2^{2n+1}-1$ 的素数之一. Tannery 相信这个定理是经验之作,它属于 Frenicle,而不属于 Fermat.

如果 p 是素数，2^p-1 是否永远是无平方因子(squarefree)的呢(它是否永远不含重因子呢)？这看来又是一个无法回答的问题．比较保险的是猜想它的答案是否定的．如果运气好的话，有可能通过计算机获得解答．正如 D. H. Lehmer 就各种因子分解方法说过的那样：“运气就是捷径．”Selfridge 把计算上的困难加以合理的考虑，提出了下面的问题：再求出 50 个像 1093 和 3511 那样的数(Fermat 定理告诉我们，如果 p 是素数，那么 p 整除 2^p-2；而数 1093 和 3511 是小于 $6\cdot10^9$ 的所有数中使 p^2 整除 2^p-2 的仅有的素数)．目前还不知道是否存在无穷多个素数 p，使 p^2 整除 2^p-2．甚至也不知道是否存在无穷多个素数 p，使 p^2 不整除 2^p-2，尽管这一结论可以从强有力的 ABC 猜想推出(见 B17)．

所谓的循环整数(repunit)，即 $(10^p-1)/9$，当 $p=2,19,23,317,1031$ 时为素数．不等于 1 的循环整数已知从不为平方数．Rotkiewicz 指出，除 1 以外的循环整数都不是立方数．它们何时为无平方因子数呢？素数 3，487 和 56598313 是小于 2^{32}的数中仅有的使 p^2 整除 10^p-10 的素数．Peter Montgomery 对 $a<100$ 和 $p<2^{32}$列出了所有使 p^2 整除 $a^{p-1}-1$ 成立的情形．

Selfridge 问道，序列(用十进制记号)

$$1,12,123,1234,12345,123456,1234567,12345678,123456789,$$
$$12345678910,1234567891011,123456789101112,\cdots$$

中是否包含无穷多个素数？在其他进位制下也可以问同样的问题．例如

$$12345610111213_7=131870666077_{10}$$

是一个素数．

Wagstaff 注意到，在小于 180 的所有数中，仅有的使 $(p^p-1)/(p-1)$ 为素数的素数是 $p=2,3,7,19,31$；使 $(p^p+1)/(p+1)$ 为素数的素数是 $p=3,5,17,157$．

人们对 Fermat 数(Fermat number) $F_n=2^{2^n}+1$ 也有持续不断的兴趣．当 $0\leqslant n\leqslant4$ 时它是素数，而对 $5\leqslant n\leqslant21$ 以及许多很大

的 n,它都是合数. Hardy 和 Wright 给出一个富有启发性的合理的讨论,认为只有有限多个 Fermat 数是素数. Selfridge 则进一步支持如下的猜想:所有其余的 Fermat 数都是合数.

人们猜想 Fermat 数都是无平方因子数. Gostin 和 Mclaughlin 曾经验证,在当时已知为合数的 71 个 Fermat 数中(对 $m=3310$, 4724 和 6537, F_m 的因子未如此予以检验),已知的 85 个因子中有 82 个因子均不重复. Wilfrid Keller 和 Hiromi Suyama 发现了 Fermat 数的一些新因子. $2^{2^m}+1$ 的形如 $k\cdot 2^n+1$ 的 88 个素因子列在"Cunningham 计划"的引言中的 p. lx 中(见下面所列出的 Brillhart 等人的文献). 在该书第二版中,该数扩大到 114 个,在本书写作时,至少已知有 150 个这样的数. Lenstra, Lenstra, Manasse 和 Pollard 已经完全分解了第九个 Fermat 数,而 R. P. Brent 则完全分解了第十一个 Fermat 数. 对大数分解有兴趣的读者可与 Samuel S. Wagstaff 联系.

由于数学家对形如 $k\cdot 2^n+1$ 的数是 Fermat 数的潜在因子这一特殊兴趣,又因为它们的素性判别较为容易,所以这样的数(至少对较小的 k)受到特别的注意. 例如, Harvey Dubner 和 Wilfrid Keller 就发现了很大的素数,1984 年由 Keller 发现的非 Fermat 素数的记录是 $(k,n)=(5,23473)$. 他的另一个发现是 $(k,n)=(289,16502)$,这个数的奇妙之处是,它可以写成(18496,18496),这是一个 Cullen 素数(B20),它还可以写作 $(17\cdot 2^{9251})^2+1$,这是一个形如 a^2+1 的素数(A1).

如我们提到的,该记录曾被一个形如 $k\cdot 2^n-1$ 的素数 $(k,n)=(391581,216193)$ 所打破,也见 B21.

Hugh Williams 发现,对 $r=3,5,7,11$ 及所有 $n\leqslant 500$, $(r-1)r^n-1$ 皆为素数:

$r=3$　$n=1,2,3,7,8,12,20,23,27,35,56,62,68,131,222,$
384, 387

$r=5$　$n=1,3,9,13,15,25,39,69,165,171,209,339$

$r=7$　$n=1,2,7,18,55,69,87,119,141,189,249,354$

$r = 11 \quad n = 1, 3, 37, 119, 255, 355, 371, 497$

我们不大可能肯定 Fibonacci 序列(Fibonacci sequence)

1,1,**2**,**3**,**5**,8,**13**,21,34,55,**89**,144,**233**,377,610,987,**1597**,…,

(其中 $u_1 = u_2 = 1$, $u_{n+1} = u_n + u_{n-1}$)包含无穷多个素数(Hugh Williams 发现 Fibonacci 数 u_{2971}是一个大素数). 类似地,对与之有关的 **Lucas 序列**(Lucas sequence)

1,**3**,4,**7**,**11**,18,**29**,**47**,76,123,**199**,322,**521**,843,1364,…,

和大多数由二阶递推公式定义的其他的 Lucas-Lehmer 序列(其中 $u_1 \perp u_2$)也有同样的问题. 然而,Graham 证明了,与

$$u_0 = 1786\ 772701\ 928802\ 632268\ 715130\ 455793$$

$$u_1 = 1059\ 683225\ 053915\ 111058\ 165141\ 686995$$

对应的序列中根本就没有素数! Knuth 注意到,Graham 的数还可以取为

$$u_0 = 331\ 635635\ 998274\ 737472\ 200656\ 430763$$

$$u_1 = 1510\ 028911\ 088401\ 971189\ 590305\ 498785;$$

他还给出了一个更小的例子

$$u_1 = 49463\ 435743\ 205655, \qquad u_2 = 62638\ 280004\ 239857.$$

Raphael Robinson 考虑了 Lucas 序列(有时称为 Pell 序列(Pell sequence))

$$u_0 = 0, \qquad u_1 = 1, \qquad u_{n+1} = 2u_n + u_{n-1},$$

并由

$$u_n = \prod_{d \mid n} L_d$$

定义了本原部分(primitive part) L_n. 他注意到 $L_7 = 13^2$, $L_{30} = 31^2$. 他问:是否有大的 n 使 L_n 为平方数?

参考文献

R. C. Archibald, *Scripta Math.*, **3**(1935) 117.

A. O. L. Atkin & N. W. Rickert, Some factors of Fermat numbers, *Abstracts Amer. Math. Soc.*, **1**(1980) 211.

P. T. Bateman, J. L. Selfridge & S. S. Wagstaff, The new Mersenne conjecture, *Amer. Math. Monthly*, **96**(1989) 125–128; *MR* **90c**:11009.

Wieb Bosma, Explicit primality criteria for $h \cdot 2^k \pm 1$, *Math. Comput.*, **61**(1993) 97–109.

R. P. Brent, Factorization of the eleventh Fermat number, *Abstracts Amer. Math. Soc.*, **10**(1989) 89T-11-73.

R. P. Brent & J. M. Pollard, Factorization of the eighth Fermat number, *Math. Comput.*, **36**(1981) 627–630; *MR* **83h**:10014.

John Brillhart & G. D. Johnson, On the factors of certain Mersenne numbers, I, II *Math. Comput.*, **14**(1960) 365–369, **18**(1964) 87–92; *MR* **23**#A832, **28**#2992.

John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman & Samuel S. Wagstaff, Factorizations of $b^n \pm 1$, $b = 2,3,5,6,7,10,11,12$ up to high powers, *Contemp. Math.*, **22**. Amer. Math. Soc., Providence RI, 1983, 1988; *MR* **84k**:10005, **90d**:11009.

John Brillhart, Peter L. Montgomery & Robert D. Silverman, Tables of Fibonacci and Lucas factorizations, *Math. Comput.*, **50**(1988) 251–260 & S1–S15.

John Brillhart, J. Tonascia & P. Weinberger, On the Fermat quotient, in *Computers in Number Theory*, Academic Press, 1971, 213–222.

W. N. Colquitt & L. Welsh, A new Mersenne prime, *Math. Comput.*, **56**(1991) 867–870; *MR* **91h**:11006.

Harvey Dubner, Generalized Fermat numbers, *J. Recreational Math.*, **18** (1985–86) 279–280.

Harvey Dubner, Generalized repunit primes, *Math. Comput.*, **61** (1993) 927–930.

John R. Ehrman, The number of prime divisors of certain Mersenne numbers, *Math. Comput.*, **21**(1967) 700–704; *MR* **36**#6368.

Donald B. Gillies, Three new Mersenne primes and a statistical theory, *Math. Comput.*, **18**(1964) 93–97; *MR* **28**#2990.

Gary B. Gostin & Philip B. McLaughlin, Six new factors of Fermat numbers, *Math. Comput.*, **38**(1982) 645–649; *MR* **83c**:10003.

R. L. Graham, A Fibonacci-like sequence of composite numbers, *Math. Mag.*, **37**(1964) 322–324; *Zbl* **125**, 21.

Richard K. Guy, The strong law of small numbers, *Amer. Math. Monthly*, **95**(1988) 697–712; *MR* **90c**:11002 (see also *Math. Mag.*, **63**(1990) 3–20; *MR* **91a**:11001.

Wilfrid Keller, Factors of Fermat numbers and large primes of the form $k.2^n + 1$, *Math. Comput.*, **41**(1983) 661–673; *MR* **85b**:11117.

Wilfrid Keller, New factors of Fermat numbers, *Abstracts Amer. Math. Soc.*, **5**(1984) 391.

Wilfrid Keller, The 17th prime of the form $5.2^n + 1$, *Abstracts Amer. Math. Soc.*, **6**(1985) 121.

Donald E. Knuth, A Fibonacci-like sequence of composite numbers, *Math. Mag.*, **63**(1990) 21–25; *MR* **91e**:11020.

M. Kraitchik, *Sphinx*, 1931, 31.

D. H. Lehmer, *Sphinx*, 1931, 32, 164.

D. H. Lehmer, On Fermat's quotient, base two, *Math. Comput.*, **36**(1981) 289–290; *MR* **82e**:10004.

A. K. Lenstra, H. W. Lenstra, M. S. Manasse & J. M. Pollard, The factorization of the ninth Fermat number, *Math. Comput.*, **61**(1993) 319–349; *MR* **93k**:11116.

Peter L. Montgomery, New solutions of $a^{p-1} \equiv 1 \bmod p^2$, *Math. Comput.*, **61**(1993) 361–363.

Thorkil Naur, New integer factorizations, *Math. Comput.*, **41**(1983) 687–695; *MR* **85c**:11123.

Rudolf Ondrejka, Titanic primes with consecutive like digits, *J. Recreational Math.*, **17**(1984-85) 268–274.

Herman te Riele, Walter Lioen & Dik Winter, Factorization beyond the googol with MPQS on a single computer, *CWI Quarterly*, 4(1991) 69–72.

A. Rotkiewicz, Note on the diophantine equation $1 + x + x^2 + \ldots + x^n = y^m$, *Elem. Math.*, **42**(1987) 76.

Daniel Shanks & Sidney Kravitz, On the distribution of Mersenne divisors, *Math. Comput.*, **21**(1967) 97–100; *MR* **36**:#3717.

Hiromi Suyama, Searching for prime factors of Fermat numbers with a microcomputer (Japanese) *bit*, **13**(1981) 240-245; *MR* **82c**:10012.

Hiromi Suyama, Some new factors for numbers of the form $2^n \pm 1$, 82T-10-230 *Abstracts Amer. Math. Soc.*, **3**(1982) 257; IV, **5**(1984) 471.

Hiromi Suyama, The cofactor of F_{15} is composite, 84T-10-299 *Abstracts Amer. Math. Soc.*, **5**(1984) 271.

Samuel S. Wagstaff, Divisors of Mersenne numbers, *Math. Comput.*, **40**(1983) 385–397; *MR* **84j**:10052.

Samuel S. Wagstaff, The period of the Bell exponential integers modulo a prime, in *Math. Comput. 1943–1993* (Vancouver, 1993), Proc. Sympos. Appl. Math., Amer. Math. Soc., 1994.

H. C. Williams, The primality of certain integers of the form $2Ar^n - 1$, *Acta Arith.*, **39**(1981) 7–17; *MR* **84h**:10012.

H. C. Williams, How was F_6 factored? *Math. Comput.*, **61**(1993) 463–474.

Samuel Yates, Titanic primes, *J. Recreational Math.*, **16**(1983-84) 265–267.

Samuel Yates, Sinkers of the Titanics, *J. Recreational Math.*, **17**(1984-85) 268–274.

Samuel Yates, Tracking Titanics, in *The Lighter Side of Mathematics*, Proc. Strens Mem. Conf., Calgary 1986, Math. Assoc. of America, Washington DC, *Spectrum* series, 1993, 349–356.

Jeff Young & Duncan Buell, The twentieth Fermat number is composite, *Math. Comput.*, **50**(1988) 261–263.

A4. 素数竞赛

一个数 a 说成是模(modulo)一个正数 b 与 c 同余(congruent)(记为 $a \equiv c \bmod b$),如果 b 是 $a-c$ 的因子. S. Chowla 曾猜想,如果 $a \perp b$,则存在无穷多对相邻素数使 $p_n \equiv p_{n+1} \equiv a \bmod b$. $b=4$,

$a=1$ 的情形可从 Littlewood 的一个定理得出. 在此情形,还给出了这种相邻素数的范围. 而 $b=4,a=3$ 的情形则由 Knapowski 和 Turán 给出证明. Turán 注意到,发现长的模 4 余 1 的素数序列是有意义的(例如与 Riemann 猜想有关). Den Haan 发现了 9 个素数

11593,11597,11617,11621,11633,11657,11677,11681,11689.

有 4 个由 10 个这样的素数组成的序列分别终止于 373777, 495461,509521 和 612217,一个由 11 个这样的素数组成的序列终止于 766373. Stephane Vandemergel 发现了不少于 16 个形如 $4k+1$ 的相邻素数,它们是 207622000+273,297,301,313,321,381, 409,417,421,489,501,517,537,549,553,561.

13个模 4 余 3 的相邻素数是 241000+603,639,643,651, 663,667679,687,691,711,727,739,771.

若 $p(b,a)$记算术级数 $a+nb$ 中的最小素数,其中 $a\perp b$,则 Linnik 证明了:存在一个常数 L(现在称为 Linnik 常数(Linnik constant)),使得有 $p(b,a)\ll b^{L}$. 潘承洞(Pan Cheng-dong),陈景润(Chen Jing-run),Matti Jutila,陈景润,Matti Jutila,S. Graham,陈景润,陈景润和刘建民(Liu Jian-Min),以及王炜(Wang Wei)相继把 L 的值改进为 5448,777,550,168,80,36,17,13.5 和 8. 最近 Heath-Brown 又得到惊人的结果 $L\leqslant 5.5$.

Elliott 和 Halberstam 证明了几乎总有

$$p(b,a)<\varphi(b)(\ln b)^{1+\delta}.$$

在其他方向上已知(见 Prachar,Schinzel 和 Pomerance 的论文):给定 a,存在无穷多个 b 的值使

$$p(b,a)>\frac{cb\ln b\ln\ln b\ln\ln\ln\ln b}{(\ln\ln\ln b)^{2}},$$

这里 c 为一个绝对常数.

Turán 对素数竞赛(prime number race)特别有兴趣. 令 $\pi(n;a,b)$表示满足 $p\leqslant n$, $p\equiv a\bmod b$ 的素数 p 的个数. 对每个适合 $a\perp b$ 的 a 和 b,是否存在无穷多个 n,使得对每个适合 $a_1\neq$

$a \bmod b$ 的 a_1 都有

$$\pi(n;a,b) > \pi(n;a_1,b)?$$

Knapowski 和 Turán 解决了一些特殊的情形，但一般情形的问题仍未获得解决.

Chebyshev 注意到，对小的 n 有 $\pi(n;1,3)<\pi(n;2,3)$ 及 $\pi(n;1,4)\leqslant\pi(n;3,4)$. Leech，以及 Shanks 和 Wrench 相互独立地发现：对 $n=26861$，第二个不等式取相反的不等号；而 Bays 和 Hudson 则发现：对位于 $n=608981813029$ 和 $n=610968213796$ 之间的多于 1 亿 5 千万个整数 n 中的每一个来说，第一个不等式都取相反的不等号.

参考文献

Carter Bays & Richard H. Hudson, The appearance of tens of billions of integers x with $\pi_{24,13}(x) < \pi_{24,1}(x)$ in the vicinity of 10^{12}, *J. reine angew. Math.*, **299/300**(1978) 234–237; *MR* **57** #12418.

Carter Bays & Richard H. Hudson, Details of the first region of integers x with $\pi_{3,2}(x) < \pi_{3,1}(x)$, *Math. Comput.*, **32**(1978) 571–576.

Carter Bays & Richard H. Hudson, Numerical and graphical description of all axis crossing regions for the moduli 4 and 8 which occur before 10^{12}, *Internat. J. Math. Sci.*, **2**(1979) 111–119; *MR* **80h**:10003.

Chen Jing-Run, On the least prime in an arithmetical progression, *Sci. Sinica*, **14**(1965) 1868–1871; *MR* **32** #5611.

Chen Jing-Run, On the least prime in an arithmetical progression and two theorems concerning the zeros of Dirichlet's L-functions, *Sci. Sinica*, **20**(1977) 529–562; *MR* **57** #16227.

Chen Jing-Run, On the least prime in an arithmetical progression and theorems concerning the zeros of Dirichlet's L-functions II, *Sci. Sinica*, **22**(1979) 859–889; *MR* **80k**:10042.

Chen Jing-Run & Liu Jian-Min, On the least prime in an arithmetic progression III, IV, *Sci. China Ser. A*, **32**(1989) 654–673, 792–807; *MR* **91h**:11090ab.

S. Graham, On Linnik's constant, *Acta Arith.*, **39**(1981) 163–179; *MR* **83d**: 10050.

Andrew Granville & Carl Pomerance, On the least prime in certain arithmetic progressions, *J. London Math. Soc.*(2), **41**(1990) 193–200; *MR* **91i**:11119.

D. R. Heath-Brown, Siegel zeros and the least prime in an arithmetic progression, *Quart. J. Math. Oxford Ser.*(2), **41**(1990) 405–418; *MR* **91m**:11073.

D. R. Heath-Brown, Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression, *Proc. London Math. Soc.*(3), **64**(1992) 265–338; *MR* **93a**:11075.

Richard H. Hudson, A common combinatorial principle underlies Riemann's formula, the Chebyshev phenomenon, and other subtle effects in comparative prime number theory I, *J. reine angew. Math.*, **313**(1980) 133–150.

Richard H. Hudson, Averaging effects on irregularities in the distribution of primes in arithmetic progressions, *Math. Comput.*, **44**(1985) 561–571; *MR* **86h**:11064.

Matti Jutila, A new estimate for Linnik's constant, *Ann. Acad. Sci. Fenn. Ser. A I No.* 471 (1970), 8*pp.*; *MR* **42** #5939.

Matti Jutila, On Linnik's constant, *Math. Scand.*, **41**(1977) 45–62; *MR* **57** #16230.

S. Knapowski & P. Turán, Über einige Fragen der vergleichenden Primzahltheorie, *Number Theory and Analysis*, Plenum Press, New York, 1969, 157–171.

S. Knapowski & P. Turán, On prime numbers ≡ 1 resp. 3 mod 4, *Number Theory and Algebra*, Academic Press, New York, 1977, 157–165; *MR* **57** #5926.

John Leech, Note on the distribution of prime numbers, *J. London Math. Soc.*, **32**(1957) 56–58.

U. V. Linnik, On the least prime in an arithmetic progression I. The basic theorem. II. The Deuring-Heilbronn phenomenon. *Rec. Math.* [*Mat. Sbornik*] *N.S.*, **15(57)**(1944) 139–178, 347–368; *MR* **6**, 260bc.

Pan Cheng-Tung, On the least prime in an arithmetic progression, *Sci. Record* (*N.S.*) **1**(1957) 311–313; *MR* **21** #4140.

Carl Pomerance, A note on the least prime in an arithmetic progression, *J. Number Theory*, **12**(1980) 218–223; *MR* **81m**:10081.

K. Prachar, Über die kleinste Primzahl einer arithmetischen Reihe, *J. reine angew. Math.*, **206**(1961) 3–4; *MR* **23** #A2399; and see Andrzej Schinzel, Remark on the paper of K. Prachar, **210**(1962) 121–122; *MR* **27** #118.

Daniel Shanks, Quadratic residues and the distribution of primes, *Math. Tables Aids Comput.*, **13**(1959) 272–284.

Wang Wei_3, On the least prime in an arithmetic progression, *Acta Math. Sinica*(**N.S.**), **7**(1991) 279–289; *MR* **93c**:11073.

A5. 素数组成的算术级数

一个仅由素数组成的算术级数可以有多长呢？表 1 给出了由 James Fry, V. A. Golubev, Andrew Moran, Paul Pritchard, S. C. Root, W. N. Seredinskii, S. Weintraub 和 Jeff Young 所发现的由 n 个素数组成的算术级数 $a, a+d, \cdots, a+(n-1)d$（有关早期的较小的发现，请见本书第一版）. 当然，公差必须以每个素数 $p \leqslant n$ 作为自己的因子（除非 $n=a$）. 猜想 n 可以任意大. 如果能够改进 Szemerédi 定理的话（见 E10），这一猜想就可得证.

更为一般地 Erdös 猜想：如果$\{a_i\}$为任一个使级数 $\sum 1/a_i$ 发散的无穷整数序列，则该序列中必包含任意长的算术级数. 他悬赏 3000 美元给证明或推翻这一猜想的人.

表 1　由素数组成的长算术级数

n	d	a	$a+(n-1)d$	source
12	30030	23143	353473	G, 1958
13	510510	766439	6892559	S, 1965
14	2462460	46883579	78895559	
16	9699690	53297929	198793279	
16	223092870	2236133941	5582526991	R, 1969
17	87297210	3430751869	4827507229	W, 1977
18	717777060	4808316343	17010526363	P
19	4180566390	8297644387	83547839407	P
19	13608665070	244290205469	489246176729	F, 1987-03
20	2007835830	803467381001	841616261771	F, 1987-03
20	7643355720	1140997291211	1286221049891	F, 1987-03
20	18846497670	214861583621	572945039351	Y&F, 1987-09-01
20	1140004565700	1845449006227	23505535754527	M&P, 1990
20	19855265430	24845147147111	25222397190281	M&P, 1990-11
21	1419763024680	142072321123	28537332814723	M&P, 1990-11-30-11

Sierpiński 定义 $g(x)$为不大于 x 的素数组成的算术级数的最大项数. 则使 $g(x)$取值为

$$g(x) = 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ \cdots$$

的对应的最小的 x 和$l(x)$是

$$l(x) = 1\ 2\ 3\ 7\ 23\ 29\ 157\ 1307\ 1669\ 1879\ 2089\ \cdots.$$

Günter Löh 找到过首项为 q、长度也为 q 的由素数组成的算术级数，例如他给出$(q,d)=(7,150)$，$(11,1536160080)$和$(13,9918821194590)$.

Pomerance 通过对点(n,p_n)描图得到了“素数图”，他证明了对每个 k 可以找到k 个素数，使它们对应的点共线.

Grosswald 指出，在如下的含义下，存在仅由殆素数(almost

prime)组成的长算术级数:有无穷多个由 k 个项组成的算术级数,它的每一项都是至多 r 个素数的乘积,这里

$$r \leqslant \lfloor k\ln k + 0.892k + 1 \rfloor.$$

他还指出,对由素数组成的有 3 项的算术级数来说,Hardy-Littlewood 估计式的阶是正确的.

参 考 文 献

P. D. T. A. Elliott & H. Halberstam, The least prime in an arithmetic progression, in *Studies in Pure Mathematics* (*Presented to Richard Rado*), Academic Press, London, 1971, 59–61; *MR* **42** #7609.

P. Erdős & P. Turán, On certain sequences of integers, *J. London Math. Soc.*, **11**(1936) 261–264.

J. Gerver, The sum of the reciprocals of a set of integers with no arithmetic progression of k terms, *Proc. Amer. Math. Soc.*, **62**(1977) 211–214.

Joseph L. Gerver & L. Thomas Ramsey, Sets of integers with no long arithmetic progressions generated by the greedy algorithm, *Math. Comput.*, **33**(1979) 1353–1359.

V. A. Golubev, Faktorisation der Zahlen der Form $x^3 \pm 4x^2 + 3x \pm 1$, *Anz. Oesterreich. Akad. Wiss. Math.-Naturwiss. Kl.*, **1969** 184–191 (see also 191–194; 297–301; **1970**, 106–112; **1972**, 19–20, 178–179).

Emil Grosswald, Long arithmetic progressions that consist only of primes and almost primes, *Notices Amer. Math. Soc.*, **26**(1979) A451.

Emil Grosswald, Arithmetic progressions of arbitrary length and consisting only of primes and almost primes, *J. reine angew. Math.*, **317**(1980) 200–208.

Emil Grosswald, Arithmetic progressions that consist only of primes, *J. Number Theory*, **14**(1982) 9–31.

Emil Grosswald & Peter Hagis, Arithmetic progressions consisting only of primes, *Math. Comput.*, **33**(1979) 1343–1352; *MR* **80k**:10054.

H. Halberstam, D. R. Heath-Brown & H.-E. Richert, On almost-primes in short intervals, in *Recent Progress in Analytic Number Theory*, Vol. 1, Academic Press, 1981, 69–101; *MR* **83a**:10075.

D. R. Heath-Brown, Three primes and an almost-prime in arithmetic progression, *J. London Math. Soc.*, (2) **23**(1981) 396–414.

D. R. Heath-Brown, Almost-primes in arithmetic progressions and short intervals, *Math. Proc. Cambridge Philos. Soc.*, **83**(1978) 357–375; *MR* **58** #10789.

Edgar Karst, 12–16 primes in arithmetical progression, *J. Recreational Math.*, **2**(1969) 214–215.

Edgar Karst, Lists of ten or more primes in arithmetical progression, *Scripta Math.*, **28**(1970) 313–317.

Edgar Karst & S. C. Root, Teilfolgen von Primzahlen in arithmetischer Progression, *Anz. Oesterreich. Akad. Wiss. Math.-Naturwiss. Kl.*, **1972**, 19–20 (see also 178–179).

Andrew Moran & Paul Pritchard, The design of a background job on a local area network, *Proc. 14th Austral. Comput. Sci. Conf.*,

Carl Pomerance, The prime number graph, *Math. Comput.*, **33**(1979) 399–408; *MR* **80d**:10013.

Paul Pritchard, Eighteen primes in arithmetic progression, *Math. Comput.*, **41** (1983) 697.

Paul Pritchard, Long arithmetic progressions of primes: some old, some new, *Math. Comput.*, **45**(1985) 263–267.

W. Sierpiński, Remarque sur les progressions arithmétiques, *Colloq. Math.*, **3** (1955) 44–49.

Sol Weintraub, Primes in arithmetic progression, *BIT* **17**(1977) 239–243.

K. Zarankiewicz, Problem 117, *Colloq. Math.*, **3**(1955) 46, 73.

A6. 算术级数中的相邻素数

有人甚至猜测:有任意长的由相邻素数组成的算术级数,如

$$251,257,263,269 \text{ 和 } 1741,1747,1753,1759.$$

Jones, Lal 和 Blundon 发现了由 5 个相邻素数组成的序列 $10^{10}+24493+30k\,(0\leqslant k\leqslant 4)$;不久 Lander 和 Parkin 找到了由 6 个这样的素数组成的序列 $121174811+30k\,(0\leqslant k\leqslant 5)$. 他们还证明了, $9843019+30k\,(0\leqslant k\leqslant 4)$是由 5 个相邻素数组成的最小的级数,在小于 $3\cdot 10^8$ 的数中还有另外 25 个这样的级数,但是没有其他长度为 6 的级数了.

还不知道在算术级数中是否存在无穷多组由 3 个相邻素数组成的集合,而 S. Chowla 在取消了对相邻素数的限制后证明了这一结论.

Hardy Nelson 发现了一个 3×3 魔方,它的 9 个元素是相邻的素数,为此他得到了 Martin Gardner 为第一个解决此问题者提供的 100 美元奖金. 当然,这些数不在一个算术级数中. 中间的那个素数是 1480028171,其余的数是这个数 ± 12, ± 18, ± 30, ± 42. 他还发现了另外 20 多个这样的魔方.

参考文献

S. Chowla, There exists an infinity of 3-combinations of primes in A.P., *Proc. Lahore Philos. Soc.*, **6** no. 2(1944) 15–16; *MR* **7**, 243.

P. Erdős & A. Rényi, Some problems and results on consecutive primes, *Simon Stevin*, **27**(1950) 115–125; *MR* **11**, 644.

M. F. Jones, M. Lal & W. J. Blundon, Statistics on certain large primes, *Math. Comput.*, **21**(1967) 103–107; *MR* **36** #3707.

L. J. Lander & T. R. Parkin, Consecutive primes in arithmetic progression, *Math. Comput.*, **21**(1967) 489.

H. L. Nelson, A consecutive prime 3 × 3 magic square, *J. Recreational Math.*

A7. Cunningham 链

证明 p 是素数的一个常用方法涉及到 $p-1$ 的因子分解. 若 $p-1=2q$,这里 q 也是一个素数,问题中的数的大小就缩小了两倍. 因此关注由每个数比它前一个数的两倍还大一的素数组成的 **Cunningham 链**(Cunningham chain)是有意义的. D. H. Lehmer 发现,恰有 3 个这样的由 7 个素数组成的链,每个链中最小的数小于 10^7:

1122659, 2245319, 4490639, 8981279, 17962559, 35925119, 71850239

2164229, 4328459, 8656919, 17313839, 34627679, 69255359, 138510719

2329469, 4658939, 9317879, 18635759, 37271519, 74543039, 149086079,

另外有两个链,其中最小的数分别是 10257809 和 10309889. $p+1$ 的分解也可被用来证明 p 是素数. Lehmer 基于 $p+1=2q$ 发现了 7 个长为 7 的链,头 3 个链中最小的数分别为 16651, 67651 和 165901. 但其中的第二个链必须除去,因为它的第五个数是 $1082401=601\times1801$(奇怪的是,它是 $2^{25}-1$ 的一个因子).

Lalout 和 Meeus 对每一种情形都发现了长为 8 的 Cunningham 链,它们分别从 19099919 和 15514861 开始,而且是该长度的链中最小的. Günter Löh 发现了许多新的链:最小的长为 9 的链,它们从 85864769 和 857095381 开始; 长为 10 的链,它们从 26089808579 和 205528443121 开始; 长为 11 的链,它们从

665043081119 和 1389122693971 开始；长为 12 的链，它们从 554688278429 和 216857744866621 开始；以及一个长为 13 的第二类链，它从 758083947856951 开始．对于长度分别为 6,7,8,9,10,起始数小于 10^{11}的第一种链的统计表明，它们相应的频数为 19991,2359,257,21 和 2.

参考文献

Claude Lalout & Jean Meeus, Nearly-doubled primes, *J. Recreational Math.*, **13** (1980/81) 30–35.

D. H. Lehmer, Tests for primality by the converse of Fermat's theorem, *Bull. Amer. Math. Soc.*, **33**(1927) 327–340.

D. H. Lehmer, On certain chains of primes, *Proc. London Math. Soc.*, **14A** (Littlewood 80 volume, 1965) 183–186.

Günter Löh, Long chains of nearly doubled primes, *Math. Comput.*, **53**(1989) 751–759; *MR* **90e**:11015.

A8．素数间隙，孪生素数

关于相邻素数的间隙有许多问题．记 $d_n = p_{n+1} - p_n$，则 $d_1 = 1$，而所有其他的 d_n 皆为偶数．d_n 能有多大和多小呢？Rankin 证明了，对无穷多个 n 有

$$d_n > \frac{c\ln n \ln\ln n \ln\ln\ln\ln n}{(\ln\ln\ln n)^2}.$$

Erdös 悬赏 5000 美元给证明或推翻下述结论的人：常数 c 可取任意大．Rankin 得到的最好的值是 $c = e^{\gamma}$，这里 γ 是 Euler 常数；Maier 和 Pomerance 将此改进为乘上一个因子 $k \approx 1.31256$，它是方程 $4/k - e^{-4/k} = 3$ 的根；Pintz 对此作了进一步的改进．

一个非常著名的猜想是孪生素数猜想，即无穷多次有 $d_n = 2$．如果 $n > 6$，在 n 和 $2n$ 之间是否必存在孪生素数？Hardy 和 Littlewood 的猜想 B(见 A1)是说，$P_k(n)$(定义为小于 n 且相差为一个偶数 k 的素数对的个数)渐近地由下述公式给出：

$$P_k(n) \sim \frac{2cn}{(\ln n)^2} \prod \left(\frac{p-1}{p-2}\right),$$

其中的乘积取过 k 的所有奇素因子(当 k 是 2 的幂时,k 的奇素因子集为空集,此时取该乘积的值为 1);而 $c=\prod(1-1/(p-1)^2)$,此乘积取过所有奇素数,因此有 $2c\approx1.32032$. 若 $\pi_{1,2}(n)$ 表示使得 $p+2$ 有至多 2 个素因子的素数 p 的个数,则 Fouvry 和 Grupp 证明了

$$\pi_{1,2}(n)\geqslant 0.71\times\frac{2cn}{(\ln n)^2},$$

数 0.71 被刘弘泉和吴杰分别改进为 1.015 和 1.05.

大孪生素数 $9\times2^{211}\pm1$ 是由 Lehmer 以及 Riesel 相互独立地发现的. Crandall 和 Penk 发现了有 64 位、136 位、154 位、203 位及 303 位的孪生素数;Williams 发现了 $156\times5^{202}\pm1$;Baillie 发现了 $297\times2^{546}\pm1$;Atkin 和 Rickert 发现了

$$694503810\times2^{2304}\pm1 \quad 和 \quad 1159142985\times2^{2304}\pm1;$$

1989 年,Brown, Noll, Parady, Smith 和 Zarantonello 发现了

$$663777\times2^{7650}\pm1,\quad 571305\times2^{7701}\pm1,\quad 1706595\times2^{11235}\pm1.$$

1993 年 8 月 16 日,Harvey Dubner 宣布了一个新的记录

$$2^{4025}\times3\times5^{4020}\times7\times11\times13\times79\times223\pm1,$$

这个数有 4030 位.

Richard Brent 对小于 10^{11}的 224376048 个素数中使 $p+2$ 也为素数的素数 p 进行了计算,其个数大约比猜想 B 给出的要多出 9%.

Bombieri 和 Davenport 证明了

$$\liminf\frac{d_n}{\ln n}<\frac{2+\sqrt{3}}{8}\approx0.46650$$

(毫不怀疑其真实结果应是 0. 自然,若孪素数猜想为真即蕴含此结论成立);G. Z. Pilt'yaĭ 将右边的常数改进为 $(2\sqrt{2}-1)/4\approx0.45711$;Uchiyama 得到 $(9-\sqrt{3})/16\approx0.454256$;Huxley 得到 $(4\sin\theta+3\theta)/(16\sin\theta)\approx0.44254$,其中 $\theta+\sin\theta=\pi/4$,后来他又改进为 0.4394;而 Helmut Maier 得到 0.248.

Huxley 还证明了

$$d_n < p_n^{7/12+\epsilon};$$

Heath-Brown 和 Iwaniec 将指数改进为 11/20; Mozzochi 得到 0.548;楼世拓(Lou Shi-tuo)和姚琦(Yao Qi)得到 6/11. Cramér 利用 Riemann 猜想证明了

$$\sum_{n<x} d_n^2 < cx(\ln x)^4.$$

Erdös 猜想上式右边可取为 $cx(\ln x)^2$,但他认为无法给出证明. 而 Riemann 猜想则蕴含 $d_n < p_n^{1/2+\epsilon}$.

Dorin Andrica 猜想对所有自然数 n 有

$$¿ \quad \sqrt{p_{n+1}} - \sqrt{p_n} < 1 \quad ?$$

Dan Grecu 对适合 $p_n < 10^6$ 的素数进行了验证. 在 Amer. Math. Monthly, 83(1976) 61 上给出了一个未解决的难题:

$$¿ \quad \lim_{n\to\infty}(\sqrt{p_{n+1}} - \sqrt{p_n}) = 0 \quad ?$$

若它为真,则对充分大的 n 就蕴含 Andrica 的猜想为真,它可以和在 A2 中提到的 Cramér 猜想相比较,也可以和下面的 Shanks 猜想做比较. Shanks 给出一个有启发意义的推理,这一推理支持下述猜想:如果 $p(g)$表示使下一个相邻素数差为 g 的第一个素数,那么就有 $\ln p(g) \sim \sqrt{g}$. Lehmer, Lander 和 Parkin, Brent, Weintraub, Young 和 Potler 以及其他人都研究过素数间隙的记录. 表 2 展示了 Shanks 的猜想.

最后一条记录是 1993 年 8 月 Aaron Potler 和 Jeff Young 告诉我们的一个未经发表的结果.

陈景润曾经证明了,对充分大的 x,对任何 $\alpha \geqslant 0.477$,区间$[x - x^\alpha, x]$中总有一个至多有两个素因子的数. Halberstam, Heath-Brown 和 Richert (见问题 A5 的文献)证明了,对 $\alpha \geqslant 0.455$,在所给区间中必有至少 $x^\alpha/121\ln x$ 个至多有两个素因子的数. 而 Iwaniec和 Laborde 进一步将指数减小到 0.45.

Victor Meally 用到术语素数荒漠(prime desert). 他注意到,在 373 以下,最常见的相邻素数间隙是 2;在 467 以下有 24 个相邻素数间隙是 2,4 和 6; 在 563 以下最常见的间隙是 6, 正如在 10^{14}和

表 2　最早的相邻素数间的大间隙

g	$p(g)$	$(\ln p)^2$	$g/(\ln p)^2$
456	25056082543	573.33	0.7953
464	42652618807	599.09	0.7745
468	127976335139	654.09	0.7155
474	182226896713	672.29	0.7051
486	241160624629	686.90	0.7075
490	297501076289	697.95	0.7021
500	303371455741	698.98	0.7153
514	304599509051	699.19	0.7351
516	416608696337	715.85	0.7208
532	461690510543	721.36	0.7375
534	614487454057	736.80	0.7247
540	738832928467	746.84	0.7230
582	1346294311331	779.99	0.7462
588	1408695494197	782.53	0.7514
602	1968188557063	801.35	0.7512
652	2614941711251	817.52	0.7975
674	7177162612387	876.27	0.7692
716	13829048560417	915.53	0.7821
766	19581334193189	936.70	0.8178
778	42842283926129	985.24	0.7897
804	90874329412297	1033.01	0.7783

$10^{14}+10^8$ 之间以及从 2 到 10^{14}之间那样.他问道:何时 30 成为最常见的相邻素数间隙? Conway 和 Odlyzko 称 d 是对 x 的一个**冠军**(champion)(记为 $C(x)$——译者注),如果它最经常性地在$\leqslant x$的数中作为相邻素数差出现.对同一个 x 可能有不止一个冠军:$C(135)=4$,$C(100)=\{2,4\}$.他们认为仅有的冠军是 4 和素数的阶乘 2,6,30,210,2310,…是否有冠军$\to\infty$? 是否每个素数 p 都整除满足 $x\geqslant x_0(p)$的所有冠军呢?

参考文献

A. O. L. Atkin & N. W. Rickert, On a larger pair of twin primes, Abstract 79T-A132, *Notices Amer. Math. Soc.*, **26**(1979) A-373.

E. Bombieri & H. Davenport, Small differences between prime numbers, *Proc. Roy. Soc. Ser. A*, **293**(1966)1–18; *MR* **33** #7314.

Richard P. Brent, The first occurrence of large gaps between successive primes, *Math. Comput.*, **27** (1973) 959–963; *MR* **48** #8360; (and see *Math. Comput.*, **35** (1980) 1435–1436.

Richard P. Brent, Irregularities in the distribution of primes and twin primes, *Math. Comput.*, **29**(1975) 43–56.

J. H. Cadwell, Large intervals between consecutive primes, *Math. Comput.*, **25** (1971) 909–913.

Chen Jing-Run, On the distribution of almost primes in an interval II, *Sci. Sinica*, **22**(1979) 253–275; *Zbl.*, 408.10030.

Chen Jing-Run & Wang Tian-Ze, , *Acta Math. Sinica*, **32**(1989) 712–718; *MR* **91e**:11108.

Chen Jing-Run & Wang Tian-Ze, On distribution of primes in an arithmetical progression, *Sci. China Ser. A*, **33**(1990) 397–408; *MR* **91k**:11078.

H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, *Acta Arith.*, **2**(1937) 23–46.

É. Fouvry & F. Grupp, On the switching principle in sieve theory, *J. reine angew. Math.*, **370**(1986) 101–126; *MR* **87j**:11092.

J. B. Friedlander & J. C. Lagarias, On the distribution in short intervals of integers having no large prime factor, *J. Number Theory*, **25**(1987) 249–273.

D. A. Goldston, On Bombieri and Davenport's theorem concerning small gaps between primes, *Mathematika*, **39**(1992) 10–17; *MR* **93h**:11102.

Glyn Harman, Short intervals containing numbers without large prime factors, *Math. Proc. Cambridge Philos. Soc.*, **109**(1991) 1–5.

Jan Kristian Haugland, Large prime-free intervals by elementary methods, *Normat*, **39**(1991) 76–77.

Martin Huxley, An application of the Fouvry-Iwaniec theorem, *Acta Arith.*, **43**(1984) 441–443.

H. Iwaniec & M. Laborde, P_2 in short intervals, *Ann. Inst. Fourier(Grenoble)*, **31**(1981) 37–56; *MR* **83e**:10061.

Jia Chao-Hua, Three primes theorem in a short interval VI (Chinese), *Acta Math. Sinica*, **34**(1991) 832–850; *MR* **93h**:11104.

Liu Hong-Quan, On the prime twins problem, *Sci. China Ser. A*, **33**(1990) 281–298; *MR* **91i**:11125.

Lou Shi-Tuo & Qi Yao, Upper bounds for primes in intervals (Chinese), *Chinese Ann. Math. Ser. A*, **10**(1989) 255–262; *MR* **91d**:11112.

Helmut Maier, Small differences between prime numbers, *Michigan Math. J.*, **35**(1988) 323–344.

Helmut Maier, Primes in short intervals, *Michigan Math. J.*, **32**(1985) 221–225.

Helmut Maier & Carl Pomerance, Unusually large gaps between consecutive primes, *Théorie des nombres*, (Quebec, PQ, 1987), de Gruyter, 1989, 625–632; *MR* **91a**:11045: and see *Trans. Amer. Math. Soc.*, **322**(1990) 201–237; *MR* **91b**:11093.

C. J. Mozzochi, On the difference between consecutive primes, *J. Number Theory* **24** (1986) 181–187.

Bodo K. Parady, Joel F. Smith & Sergio E. Zarantonello, Largest known twin primes, *Math. Comput.*, **55**(1990) 381–382; *MR* **90j**:11013.

Г. З. Пильтяй, О величине разности между соседними простыми числами, Исследования по теории чисел, вып. 4, Издательство Саратовского университета 1972, 73–79.

Daniel Shanks, On maximal gaps between successive primes, *Math. Comput.*, **18**(1964) 646–651; *MR* **29** #4745.

S. Uchiyama, On the difference between consecutive prime numbers, *Acta Arith.*, **27** (1975) 153–157.

Jie Wu, Sur la suite des nombres premiers jumeaux, *Acta Arith.*, **55**(1990) 365–394; *MR* **91j**:11074.

Jeff Young & Aaron Potler, First occurrence prime gaps, *Math. Comput.*, **52**(1989) 221–224.

Alessandro Zaccagnini, A note on large gaps between consecutive primes in arithmetic progressions, *J. Number Theory*, **42**(1992) 100–102.

A9. 素数类型

比 Chowla 猜想(见 A4)更为一般的一个猜想是说:只要没有同余关系排斥它们,任何给定类型的连续素数集都有无穷多个.例如,看来像是存在无穷多个素数三元组

$$\{6k-1, 6k+1, 6k+5\} \text{ 和 } \{6k+1, 6k+6, 6k+7\}.$$

这可能会比孪生素数猜想更难解决,不过它的貌似合理性很有意思,因为 Hensley 和 Richards 已经证明了它与著名的猜想(也属于 Hardy 和 Littlewood)

$$¿¿¿\quad \pi(x+y) \leqslant \pi(x) + \pi(y) \quad ???$$

(对所有整数 $x, y \geqslant 2$ 成立)矛盾.由于此式很像是错的,我们要围绕它提出比平常更多的问题.确实有希望找到与该不等式结论矛盾的 x 和 y 的值,不过还有另一个猜想

$$¿\quad \pi(x+y) \leqslant \pi(x) + 2\pi(y/2) \quad ?$$

Hensley 和 Richards 的方法对它不再适用.

Montgomery 和 Vaughan 证明了有

$$\pi(x+y)-\pi(x)\leqslant 2y/\ln y;$$

Iwaniec 注意到对每个 $\theta(0<\theta<1)$ 存在一个 $\eta(\theta)>\theta$,使得对充分大的 x 有

$$\pi(x+x^{\theta})-\pi(x)<(2+\varepsilon)x^{\theta}/(\eta(\theta)\ln x);$$

他发现对 $\theta>\frac{1}{3}$ 有 $\eta(\theta)=\frac{5}{3}\theta-\frac{2}{9}$,对 $\theta>\frac{1}{2}$ 有 $\eta(\theta)=(1+\theta)/2$.楼世拓和姚琦对此做了部分改进,他们得到:对 $\frac{6}{11}<\theta\leqslant\frac{11}{20}$ 有 $\eta(\theta)=(100\theta-45)/11$.

C. W. Trigg 报告说,1978 年 M. A. Penk 发现了 4 个素数 p, $p+2$, $p+6$ 和 $p+8$,其中

$$p=802359150003121605557551380867519560344356971.$$

H. F. Smith 注意到,类型 11,13,17,19,23,29,31,37 至少重复了 3 次,这 3 次开头的素数分别是 15760091,25658841 和 93625991.但无论在哪种情形,都没有与 41 对应的素数,虽然对 $n=88830$和 855750, $n-11$, $n-13$, $\cdots$, $n-41$ 全都是素数.

Leech 给出一个未解决的问题:找 33 个大于 11 的连续数,使其中有 10 个素数.1961 年 Herschel Smith 找到了 20 个这样的集合以及 5 个有 37 个连续整数且包含 11 个素数的例子. Smith 写道,Selfridge 发现了他 1957 年的论文中的某些错误. Sten Säfholm 发现了素数集($n=33081664140$)

$$\{n+11,\cdots,n+43\},$$

并且还重新发现了 Smith 的前 3 个例子:对 $n=9853497780$, 21956291910 和 22741837860,集合

$$\{n-11,\cdots,n-43\}$$

中每个数都是素数. Leech 想知道为什么后一情形似乎比前一情形更容易发生? 我猜想这是素数类型(见 A4)的一个更为复杂的表述方式;在我看来,借助于更为强大的工具,我们会看到差额得到补偿(无穷多次). Dimitrios Betsis 和 Sten Säfholm 发现了更多的

类型，他最终得到素数集 $\{n+11, \cdots, n+61\}$（对 $n=21817283854511250$）及素数集 $\{n-11, \cdots, n-61\}$（对 $n=79287805466244270$）.

Erdös 问：对每个 k，使 $p_k, p_{k+1}, \cdots, p_{k+l-1}$ 是此种类型中惟一一个仅有 l 个相连素数集合的最小的 l 是什么？例如，类型 3，5，7 不可能再次出现；类型 5，7，11，13，17 在 101，103，107，109，113 中得到重复，而且这种类型无疑会出现无穷多次；但对模 5 的考虑表明，类型 5，7，11，13，17，19 不会再出现 $(p_k, l)=(2,2),(3,3),(5,6)\cdots$.

参考文献

Antal Balog, The prime k-tuplets conjecture on the average, *Analytic Number Theory (Allerton Park, IL,* 1989), 47–75, *Progr. Math.*, **85**, Birkhäuser, Boston, 1990.

Paul Erdős & Ian Richards, Density functions for prime and relatively prime numbers, *Monatsh. Math.*, **83**(1977) 99–112; *Zbl.* **355**.10034.

John B. Friedlander & Andrew Granville, Limitations to the equi-distribution of primes I, IV, III, *Ann. of Math.*(2), **129**(1989) 363–382; *MR* **90e**:11125; *Proc. Roy. Soc. London Ser. A*, **435**(1991) 197–204; *MR* **93g**:11098; *Compositio Math.*, **81**(1992) 19–32.

John B. Friedlander, Andrew Granville, Adolf Hildebrandt & Helmut Maier, Oscillation theorems for primes in arithmetic progressions and for sifting functions, *J. Amer. Math. Soc.*, **4**(1991) 25–86; *MR* **92a**:11103.

Douglas Hensley & Ian Richards, On the incompatibility of two conjectures concerning primes, *Proc. Symp. Pure Math.*, (Analytic Number Theory, St. Louis, 1972) **24** 123–127.

H. Iwaniec, On the Brun-Titchmarsh theorem, *J. Math. Soc. Japan*, **34**(1982) 95–123; *MR* **83a**:10082.

John Leech, Groups of primes having maximum density, *Math. Tables Aids Comput.*, **12**(1958) 144–145; *MR* **20** #5163.

H. L. Montgomery & R. C. Vaughan, The large sieve, *Mathematika*, **20**(1973) 119–134; *MR* **51** #10260.

Ian Richards, On the incompatibility of two conjectures concerning primes; a discussion of the use of computers in attacking a theoretical problem, *Bull. Amer. Math. Soc.*, **80**(1974) 419–438.

Herschel F. Smith, On a generalization of the prime pair problem, *Math. Tables Aids Comput.*, **11**(1957) 249–254; *MR* **20** #833.

Charles W. Trigg, A large prime quadruplet, *J. Recreational Math.*, **14** (1981/82) 167.

Sheng-Gang Xie, The prime 4-tuplet problem (Chinese. English summary), *Sichuan Daxue Xuebao*, **26**(1989) 168–171; *MR* **91f**:11066.

A10. Gilbreath 猜想

由 $d_n^1=d_n$ 以及 $d_n^{k+1}=|d_{n+1}^k-d_n^k|$ 来定义 d_n^k，这就是素数序列的连续的绝对差(图 2). N. L. Gilbreath 猜想(Hugh Williams 注意到很久以前 Proth 声称证明了)对所有 k 有 $d_1^k=1$. Killgrove 和 Ralston 对 $k<63419$ 作了验证. Odlyzko 对直到 $\pi(10^{13})\approx 3\cdot 10^{11}$ 的素数作了验证，他只需要检查前 635 个差.



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89
1	2	2	4	2	4	2	4	6	2	6	4	2	4	6	6	2	6	4	2	6	4	6	
1	0	2	2	2	2	2	2	4	4	2	2	2	2	0	4	4	2	2	4	2	2		
1	2	0	0	0	0	0	2	0	2	0	0	0	2	4	0	2	0	2	2	0			
1	2	0	0	0	0	2	2	2	2	0	0	2	2	4	2	2	2	0	2				
1	2	0	0	0	2	0	0	0	2	0	2	0	2	2	0	0	2	2					
1	2	0	0	2	2	0	0	2	2	2	2	2	0	2	0	2	0						
1	2	0	2	0	2	0	2	0	0	0	0	2	2	2	2	2							
1	2	2	2	2	2	2	2	0	0	0	2	0	0	0	0								
1	0	0	0	0	0	0	2	0	0	2	2	0	0	0									

图 2　素数序列的连续绝对差

Hallard Croft 和其他人认为并不像上面说的那样，这其实与素数没有什么关系，但是对由 2 和奇数组成的任何序列来说结论是正确的，这些序列增长得不太快，或者有太大的间隙. Odlyzko 对此作了讨论.

参考文献

R. B. Killgrove & K. E. Ralston, On a conjecture concerning the primes, *Math. Tables Aids Comput.*, **13**(1959) 121–122; *MR* **21** #4943.

Andrew M. Odlyzko, Iterated absolute values of differences of consecutive primes, *Math. Comput.*, **61**(1993) 373–380; *MR* **93k**:11119.

F. Proth, Sur la série des nombres premiers, *Nouv. Corresp. Math.*, **4**(1878) 236–240.

A11. 递增和递减的素数间隙

由于素数所占的比例逐渐减小，虽然没有什么规律，但无穷多次有 $d_m < d_{m+1}$；Erdös 和 Turán 还证明了，$d_n > d_{n+1}$ 也无穷多次成立. 他们还证明了，使 $d_n > d_{n+1}$ 成立的 n 的值有正的下密度，但是尚不知道对三个连续的 d_n 的值是否也存在无穷多个递减或者递增的集合. 如若不然，则有一个 n_0 存在，对每个 i 和 $n > n_0$ 有 $d_{n+2i} > d_{n+2i+1}$ 及 $d_{n+2i+1} < d_{n+2i+2}$. Erdös 为给出这样的 n_0 不存在的证明悬赏 100 美元. 他和 Turán 甚至不能证明如下结论：对 $k > k_0$，$(-1)^r(d_{k+r+1} - d_{k+r})$ 不可能永远有同样的符号.

参 考 文 献

P. Erdős, On the difference of consecutive primes, *Bull. Amer. Math. Soc.*, **54**(1948) 885–889; *MR* **10**, 235.

P. Erdös & P. Turán, On some new questions on the distribution of prime numbers, *Bull. Amer. Math. Soc.*, **54**(1948) 371–378; *MR* **9**, 498.

A12. 伪素数，Euler 伪素数，强伪素数

Pomerance, Selfridge 和 Wagstaff 称满足 $a^{n-1} \equiv 1 \bmod n$ 的奇合数 n 为**以 a 为底的伪素数**(pseudoprime to base a)(psp(a)). 使用这一术语可以避免充斥于文献中的繁琐用语"复合的伪素数". 对每个与 n 互素的 a 都是 psp(a)的合数 n 叫做 Carmichael 数(Carmichael number)(见 A13). 一个奇合数 n 称为**以 a 为底的 Euler 伪素数**(Euler pseudoprime to base a)(epsp(a))，如果 $a \perp n$ 且 $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n$，这里 $\left(\frac{a}{n}\right)$ 是 Jacobi 符号(见 F5). 最后，一个满足 $n-1 = d \cdot 2^s$(d 为奇数)的奇合数 n 称为**以 a 为底的强伪素数**(strong pseudoprime to base a)(spsp(a))，如果有 $a^d \equiv 1 \bmod n$(否则就对某个满足 $0 \leqslant r < s$ 的 r 有 $a^{d \cdot 2^r} \equiv -1 \bmod n$). 这

些定义均用文氏图(图 3)予以描述,它展示出每个集合的最小成员.

psp(2)

Carmichael 数

epsp(2)

spsp(2)

2047 15841

1905 561

2821

341

图 3 各种 psps 集合之间的关系和每个集合中的最小元素

下面给出的 $P_2(x)$,$E_2(x)$,$S_2(x)$以及 $C(x)$的值(它们分别表示小于 x 的 psp(2),epsp(2),spsp(2)以及 Carmichael 数的个数)是由 Pomerance, Selfridge 和 Wagstaff 给出的:

x	10^3	10^4	10^5	10^6	10^7	10^8	10^9	10^{10}	$2.5\cdot 10^{10}$
$P_2(x)$	3	22	78	245	750	2057	5597	14884	21853
$E_2(x)$	1	12	36	114	375	1071	2939	7706	11347
$S_2(x)$	0	5	16	46	162	488	1282	3291	4842
$C(x)$	1	7	16	43	105	255	646	1547	2163

Lehmer 和 Erdös 指出,对充分大的 x 有

$$c_1\ln x < P_2(x) < x\exp\{-c_2(\ln x\ln\ln x)^{1/2}\},$$

而 Pomerance 将它改进为

$$\exp\{(\ln x)^{5/14}\} < P_2(x) < x\exp\{(-\ln x\ln\ln\ln x)/2\ln\ln x\},$$

他还通过一种合理的讨论得知 $P_2(x)$的真实的估计式是在上界中去掉数 2. 利用 Friedlander 的一个结果,Pomerance 把指数 5/14 改进为 85/207.

还有一些像 $2^n \equiv 2 \bmod n$ 这样的关于偶数的例子. Lehmer 发现了 $161038 = 2 \cdot 73 \cdot 1103$,而 Beeger 指出有无穷多个这样的数. 如果 F_n 表示 Fermat 数 $2^{2^n}+1$,Cipolla 证明了:如果 $k>1$ 且 $n_1<n_2<\cdots<n_k<2^{n_1}$,那么 $F_{n_1}F_{n_2}\cdots F_{n_k}$ 是一个 psp(2).

如果 $P_n^{(a)}$ 是第 n 个 psp(a),Szymiczek 证明了级数 $\sum 1/P_n^{(2)}$ 收敛,而 Mąkowski 证明了 $\sum 1/\ln P_n^{(a)}$ 发散. Rotkiewicz 有一本有关伪素数的小册子,它包含 58 个问题和 20 个猜想.

例如,其中的问题 # 22 问是否有形如 2^N-2 的伪素数. Wayne McDaniel 用 $N=465794$ 对此问题给出了肯定的回答. Rotkiewicz 指出,同余式 $2^{n-2} \equiv 1 \bmod n$ 有无穷多个合数解 n. 申茂功(Shen Mok-kong)找到 5 个这样的小于一百万的数,每个数均以 7 结尾. McDaniel 和张明志(Zhang Ming-zhi)给出例子 $73 \cdot 48544121$ 和 $524287 \cdot 13264529$,每个例子表明 3 也是可能的末位数字.

Selfridge, Wagstaff 和 Pomerance 悬赏 500 + 100 + 20 美元求一个模 10 与 3 或 7 同余的合数 n,它整除 2^n-2 和 Fibonacci 数 u_{n+1}(见 A3);或提供 20 + 100 + 500 美元给证明这种 n 不存在的人.

申茂功指出,有无穷多个 k 使方程 $2^{n-k} \equiv 1 \bmod n$ 有无穷多个合数解 n. Kiss 和 Phong 证明了,对所有 $k \geqslant 2$ 及所有 $a \geqslant 2$(a 代替原来的 2)此结论依然成立.

参考文献

Steven Arno, A note on Perrin pseudoprimes, *Math. Comput.*, **56**(1991) 371–376; *MR* **91k**:11011.

N. G. W. H. Beeger, On even numbers m dividing 2^m-2, *Amer. Math. Monthly*, **58**(1951) 553–555; *MR* **13**, 320.

R. D. Carmichael, On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$, *Amer. Math. Monthly*, **19**(1912) 22–27.

M. Cipolla, Sui numeri composti P che verificiano la congruenza di Fermat, $a^{P-1} \equiv 1 \pmod P$, *Annali di Matematica*, **9**(1904) 139–160.

P. Erdős, On the converse of Fermat's theorem, *Amer. Math. Monthly*, **56** (1949)

623–624; *MR* **11**, 331.

P. Erdős, On almost primes, *Amer. Math. Monthly*, **57**(1950) 404–407; *MR* **12**, 80.

P. Erdős, P. Kiss & A. Sárközy, A lower bound for the counting function of Lucas pseudoprimes, *Math. Comput.*, **51**(1988) 259–279; *MR* **89e**:11011.

P. Erdős & C. Pomerance, The number of false witnesses for a composite number, *Math. Comput.*, **46**(1986) 259–279; *MR* **87i**:11183.

J. B. Friedlander, Shifted primes without large prime factors, in *Number Theory and Applications*, (Proc. NATO Adv. Study Inst., Banff, 1988), Kluwer, Dordrecht, 1989, 393–401.

Daniel M. Gordon & Carl Pomerance, The distribution of Lucas and elliptic pseudoprimes, *Math. Comput.*, **57**(1991) 825–838; *MR* **92h**:11081; corrigendum **60**(1993) 877; *MR* **93h**:11108.

S. Gurak, Pseudoprimes for higher-order linear recurrence sequences, *Math. Comput.*, **55**(1990) 783–813.

Gerhard Jaeschke, On strong pseudoprimes to several bases, *Math. Comput.*, **61**(1993) 915–926.

I. Joó, On generalized Lucas pseudoprimes, *Acta Math. Hungar.*, **55**(1990) 315–322.

I. Joó & Phong Bui-Minh, On super Lehmer pseudoprimes, *Studia Sci. Math. Hungar.*, **25**(1990) 121–124; *MR* **92d**:11109.

Kim Su-Hee & Carl Pomerance, The probability that a random probable prime is composite, *Math. Comput.*, **53**(1989) 721–741; *MR* **90e**:11190.

Péter Kiss & Phong Bui-Minh, On a problem of A. Rotkiewicz, *Math. Comput.*, **48**(1987) 751–755; *MR* **88d**:11004.

D. H. Lehmer, On the converse of Fermat's theorem, *Amer. Math. Monthly*, **43**(1936) 347–354; II **56**(1949) 300–309; *MR* **10**, 681.

Andrzej Mąkowski, On a problem of Rotkiewicz on pseudoprime numbers, *Elem. Math.*, **29**(1974) 13.

A. Mąkowski & A. Rotkiewicz, On pseudoprime numbers of special form, *Colloq. Math.*, **20**(1969) 269–271; *MR* **39** #5458.

Wayne L. McDaniel, Some pseudoprimes and related numbers having special forms, *Math. Comput.*, **53**(1989) 407–409; *MR* **89m**:11006.

Carl Pomerance, A new lower bound for the pseudoprime counting function, *Illinois J. Math.*, **26**(1982) 4–9; *MR* **83h**:10012.

Carl Pomerance, On the distribution of pseudoprimes, *Math. Comput.*, **37** (1981) 587–593; *MR* **83k**:10009.

Carl Pomerance, Two methods in elementary analytic number theory, in *Number Theory and Applications*, (Proc. NATO Adv. Study Inst., Banff, 1988), Kluwer, Dordrecht, 1989, 135–161.

Carl Pomerance, John L. Selfridge & Samuel S. Wagstaff, The pseudoprimes to $25 \cdot 10^9$, *Math. Comput.*, **35**(1980) 1003–1026; *MR* **82g**:10030.

A. Rotkiewicz, *Pseudoprime Numbers and their Generalizations*, Student Association of the Faculty of Sciences, Univ. of Novi Sad, 1972; *MR* **48** #8373; *Zbl.* 324.10007.

A. Rotkiewicz, Sur les diviseurs composés des nombres $a^n - b^n$, *Bull. Soc. Roy. Sci. Liège*, **32**(1963) 191–195; *MR* **26** #3645.

A. Rotkiewicz, Sur les nombres pseudopremiers de la forme $ax + b$, *Comptes Rendus Acad. Sci. Paris*, **257**(1963) 2601–2604; *MR* **29** #61.
A. Rotkiewicz, Sur les formules donnant des nombres pseudopremiers, *Colloq. Math.*, **12**(1964) 69–72; *MR* **29** #3416.
A. Rotkiewicz, Sur les nombres pseudopremiers de la forme $nk+1$, *Elem. Math.*, **21**(1966) 32–33; *MR* **33** #112.
A. Rotkiewicz, On Euler-Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters L, Q in arithmetic progressions, *Math. Comput.*, **39** (1982) 239–247; *MR* **83k**:10004.
A. Rotkiewicz, On the congruence $2^{n-2} \equiv 1 (\bmod n)$, *Math. Comput.*, **43** (1984) 271–272; *MR* **85e**:11005.
Shen Mok-Kong, On the congruence $2^{n-k} \equiv 1 (\bmod n)$, *Math. Comput.*, **46**(1986) 715–716; *MR* **87e**:11005.
K. Szymiczek, On prime numbers p, q and r such that pq, pr and qr are pseudoprimes, *Colloq. Math.*, **13**(1964–65) 259–263; *MR* **31** #4757.
K. Szymiczek, On pseudoprime numbers which are products of distinct primes, *Amer. Math. Monthly*, **74**(1967) 35–37; *MR* **34** #5746.
S. S. Wagstaff, Pseudoprimes and a generalization of Artin's conjecture, *Acta Arith.*, **41**(1982) 151–161; *MR* **83m**:10004.
Masataka Yorinaga, Search for absolute pseudoprime numbers (Japanese), *Sûgaku*, **31** (1979) 374–376; *MR* **82c**:10008.

A13. Carmichael 数

Carmichael 数(对与合数 n 互素的所有 a 皆为 psp(a)的数)必为至少 3 个奇素因子的乘积. 早在 1899 年 Korselt 就给出了 n 为 Carmichael 数的一个充分必要条件,即,n 无平方因子且对每个整除 n 的 p 均有 $(p-1)|(n-1)$. 最小的例子是 $561 = 3 \cdot 11 \cdot 17$. 更一般地,如果 $p = 6k+1$, $q = 12k+1$ 和 $r = 18k+1$ 均为素数,则 pqr 就是一个 Carmichael 数. 看起来似乎肯定有无穷多组这样的三元素数组,但却无法证明它. Alford, Granville 以及 Pomerance (用不同的方法!)证明了有无穷多个 Carmichael 数. 事实上对充分大的 x,小于 x 的 Carmichael 数有多于 x^β 个,这里

$$\beta = \frac{5}{12}\left(1 - \frac{1}{2\sqrt{e}}\right) > 0.290306 > \frac{2}{7}.$$

Erdös 曾猜想,当 x 趋于无穷时有 $(\ln C(x))/\ln x \to 1$,他改进了 Knödel 的一个结果,由此他证明了

$$C(x) < x\exp\{-c\ln x\ln\ln\ln x/\ln\ln x\}.$$

此后 Pomerance, Selfridge 和 Wagstaff(见 A12)证明了可取 $c=1-\varepsilon$,并给出一个启发式的合理讨论,它支持下述猜想:对 $c=2+\varepsilon$,相反的不等式成立.

他们发现了 2163 个小于 $25\cdot 10^9$ 的 Carmichael 数;Jaeschke 又发现了 6075 个位于 $25\cdot 10^9$ 和 10^{12}之间的 Carmichael 数,其中 7 个有 8 个素因子. Richard Pinch 分别计算出了

$$< 10^{12} \quad 10^{13} \quad 10^{14} \quad 10^{15} \quad 10^{16}$$

的

$$8241 \quad 19279 \quad 44706 \quad 105212 \quad 246683$$

个 Carmichael 数. 一个中等大小的 Carmichael 数的例子是

$$2013745337604001 = 17\cdot 37\cdot 41\cdot 131\cdot 251\cdot 571\cdot 4159.$$

J.R. Hill 发现了大 Carmichael 数 pqr,其中 $p=5\cdot 10^{19}+371$, $q=2p-1$,而 $r=1+(p-1)(q+2)/433$. Wagstaff 造出一个有 321 位的 Carmichael 数, Woods 和 Huenemann 找到一个有 432 位的数. Dubner 继续打破这一记录以及他自己的记录,他得到一个 3710 位的 Carmichael 数 $N=PQR$,其中 $P=6M+1$, $Q=12M+1$ 和 $R=1+(PQ-1)/X$ 均为素数, $M=(TC-1)^A/4$, T 是直到 47 的所有奇素数的乘积, $C=141847$, $A=41$,而 $X=123165$. 然而 Günter Löh 和 Wolfgang Niebuhr 已经发展出新的算法,由此可以造出一个有不少于 1101518 个素因子的 Carmichael 数,(它有 16142049 位数字!)从而使以前的记录黯然失色.

Alford, Granville 和 Pomerance 证明了,存在无穷多个满足很强条件的 Carmichael 数:由 $p\mid n$ 就有 $(p^2-1)\mid(n-1)$,但是他们不知道任何这样的例子. Sid Graham 发现了 18 个这样的数,其中最小的是

$$5893983289990395334700037072001$$
$$=29\cdot 31\cdot 37\cdot 43\cdot 53\cdot 67\cdot 79\cdot 89\cdot 97\cdot 151\cdot 181\cdot 191\cdot 419\cdot 881\cdot 883$$

Richard Pinch 发现了所有这种数中最小的数是

$$443372888629441 = 17\cdot 31\cdot 41\cdot 43\cdot 89\cdot 97\cdot 167\cdot 331.$$

Graham 找到了另外 17 个数，它们满足较弱的条件 $\frac{p^2-1}{2} \mid (n-1)$.

参考文献

W. Red Alford, Andrew Granville & Carl Pomerance, *Ann. of Math.* (to appear; 1992 preprint).

Robert Baillie & Samuel S. Wagstaff, Lucas pseudoprimes, *Math. Comput.*, **35** (1980) 1391–1417.

N. G. W. H. Beeger, On composite numbers n for which $a_{n-1} \equiv 1 \bmod n$ for every a prime to n, *Scripta Math.*, **16**(1950) 133–135.

R. D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.*, **16**(1909–10) 232–238.

Harvey Dubner, A new method for producing large Carmichael numbers, *Math. Comput.*, **53**(1989) 411–414; *MR* **89m**:11013.

H. J. A. Duparc, On Carmichael numbers, *Simon Stevin*, **29**(1952) 21–24; *MR* **14**, 21f.

P. Erdős, On pseudoprimes and Carmichael numbers, *Publ. Math. Debrecen*, **4**(1956) 201–206; *MR* **18**, 18.

Andrew Granville, Prime testing and Carmichael numbers, *Notices Amer. Math. Soc.*, **39**(1992) 696–700.

D. Guillaume, Table de nombres de Carmichael inférieurs à 10^{12}, preprint, May 1991.

Jay Roderick Hill, Large Carmichael numbers with three prime factors, Abstract 79T-A136, *Notices Amer. Math. Soc.*, **26**(1979) A-374.

Gerhard Jaeschke, The Carmichael numbers to 10^{12}, *Math. Comput.*, **55** (1990) 383–389; *MR* **90m**:11018.

I. Joó & Phong Bui-Minh, On super Lehmer pseudoprimes, *Studia Sci. Math. Hungar.*, **25**(1990) 121–124.

W. Keller, The Carmichael numbers to 10^{13}, *Abstracts Amer. Math. Soc.*, **9**(1988) 328–329.

W. Knödel, Eine obere Schranke für die Anzahl der Carmichaelschen Zahlen kleiner als x, *Arch. Math.*, **4**(1953) 282–284; *MR* **15**, 289 (and see *Math. Nachr.*, **9**(1953) 343–350).

A. Korselt, Problème chinois, *L'intermédiaire des math.*, **6**(1899) 142–143.

D. H. Lehmer, Strong Carmichael numbers, *J. Austral. Math. Soc. Ser. A*, **21** (1976) 508–510.

G. Löh, Carmichael numbers with a large number of prime factors, *Abstracts Amer. Math. Soc.*, **9**(1988) 329; II (with W. Niebuhr) **10**(1989) 305.

Günter Löh & Wolfgang Niebuhr, New algorithms for constructing large Carmichael numbers, (92-11-01 preprint).

R. G. E. Pinch, The Carmichael numbers up to 10^{15}, *Math. Comput.*, **61** (1993) 381–391; *MR* **93m**:11137.

A. J. van der Poorten & A. Rotkiewicz, On strong pseudoprimes in arithmetic progressions, *J. Austral. Math. Soc. Ser. A*, **29**(1980) 316–321.

S. S. Wagstaff, Large Carmichael numbers, *Math. J. Okayama Univ.*, **22** (1980) 33–41; *MR* **82c**:10007.

H. C. Williams, On numbers analogous to Carmichael numbers, *Canad. Math. Bull.*, **20**(1977) 133–143.

Dale Woods & Joel Huenemann, Larger Carmichael numbers, *Comput. Math. Appl.*, **8**(1982) 215–216; *MR* **83f**:10017.

Masataka Yorinaga, Numerical computation of Carmichael numbers, I, II, *Math. J. Okayama Univ.*, **20**(1978) 151–163, **21**(1979) 183–205; *MR* **80d**:10026, **80j**:10002.

Masataka Yorinaga, Carmichael numbers with many prime factors, *Math. J. Okayama Univ.*, **22**(1980) 169–184; *MR* **81m**:10018.

Zhang Ming-Zhi, A method for finding large Carmichael numbers, *Sichuan Daxue Xuebao*, **29**(1992) 472–479; *MR* **93m**:11009.

A14. "好"素数和素数图

Erdös 和 Straus 称一个素数 p_n 是"**好的**(good)",如果对所有 $i(1\leqslant i\leqslant n-1)$ 有 $p_n^2>p_{n-1}p_{n+1}$,例如 5,11,17 和 29 都是"好"素数. Pomerance 用"素数图"(见 A5)说明了有无穷多个好素数. 他提出下面的问题:使 p_n 为好素数的 n 的集合是否密度为 0? 是否存在无穷多个 n,对所有 $i(1\leqslant i\leqslant n-1)$有 $p_np_{n+1}>p_{n-i}p_{n+1+i}$? 是否存在无穷多个 n,对所有 $i(1\leqslant i\leqslant n-1)$有 $p_n+p_{n+1}>p_{n-i}+p_{n+1+i}$? 又对所有 $i(1\leqslant i\leqslant n-1)$满足 $2p_n<p_{n-1}+p_{n+i}$的所有 n 的集合是否密度为 0(Pomerance 证明了有无穷多个这样的 n)? 是否有 $\limsup\{\min_{0<i<n}(p_{n-i}+p_{n+i})-2p_n\}=\infty$?

A15. 同余的相邻素数乘积

Erdös 在一封写于 1979 年 10 月 31 日的信中注意到有 $3\cdot4\equiv5\cdot6\cdot7\equiv1\bmod 11$,他提出求最小的素数 p,对于它存在整数 a,k_1,k_2,k_3 使有

$$\prod_{i=1}^{k_1}(a+i)\equiv\prod_{i=1}^{k_2}(a+k_1+i)$$

$$\equiv \prod_{i=1}^{k_3}(a+k_1+k_2+i)\equiv 1 \mod p.$$

他认为,对任意多个这样的同余乘积都存在这样的素数 p.

Mąkowski 给出下表中(与 F11 比较)与 $n=5$ 及 6 对应的例子,并说指数表可以用来发现其他的例子. W. Narkiewicz 也给出这些例子,同时还给出下表中与 $n=7,8,9$ 对应的结果. Landon Noll 和 Chuck Simmons 对此问题稍加推广,他们提出求

$$q_1!\equiv q_2!\equiv\cdots\equiv q_n! \mod p$$

的解,还给出使有 n 个项的同余方程有解的最小素数 p.

n	p	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	q_9	q_{10}	q_{11}
1	2	0										
2	2	0	1									
3	5	0	1	3								
4	17	0	1	5	11							
5	17	0	1	5	11	15						
6	23	0	1	4	8	11	21					
7	71	8	10	20	52	62	64	71				
8	599	29	51	123	184	251	290	501	540			
9	599	29	51	123	184	251	290	501	540	556		
10	3011	0	1	611	723	749	805	2205	2261	2287	2399	
11	3011	0	1	611	723	749	805	2205	2261	2287	2399	3009

参考文献

Andrzej Mąkowski, On a number-theoretic problem of Erdős, *Elem. Math.*, **38** (1983) 101–102.

A16. Gauss 素数,Eisenstein-Jacobi 素数

可以在有理数域以外的域中定义素数. 复数域中的素数称为 Gauss 素数(Gaussian prime). 可以对 Gauss 素数系统地复述与通常的素数同样的问题.

Gauss 整数(Gaussian integer) $a+bi$ (其中 a,b 是整数, $i^2=$

-1)的性状与普通整数相似：它也有惟一分解(unique factorization)(除去因子的次序、单位(unit) ± 1 和 $\pm i$ 以及相伴元(associate)以外分解式惟一，例如 7 的相伴元是 $7, -7, 7i$ 和 $-7i$). 在 Gauss 整数环中形如 $4k-1$ 的素数$(3,7,11,19,23,\cdots)$仍为素数，但其他通常的素数则可分解成 Gauss 素数：

$$2=(1+i)(1-i),\ 5=(2+i)(2-i)=-(2i-1)(2i+1),$$
$$13=(2+3i)(2-3i),\quad 17=(4+i)(4-i),$$
$$29=(5+2i)(5-2i),\ \cdots$$

Gauss 素数 $\pm 1\pm i, \pm 1\pm 2i, \pm 2\pm i, \pm 3, \pm 3i, \pm 2\pm 3i, \pm 3\pm 2i, \pm 4\pm i, \pm 1\pm 4i, \pm 5\pm 2i, \pm 2\pm 5i, \cdots$ 画在 Argand 图上形成

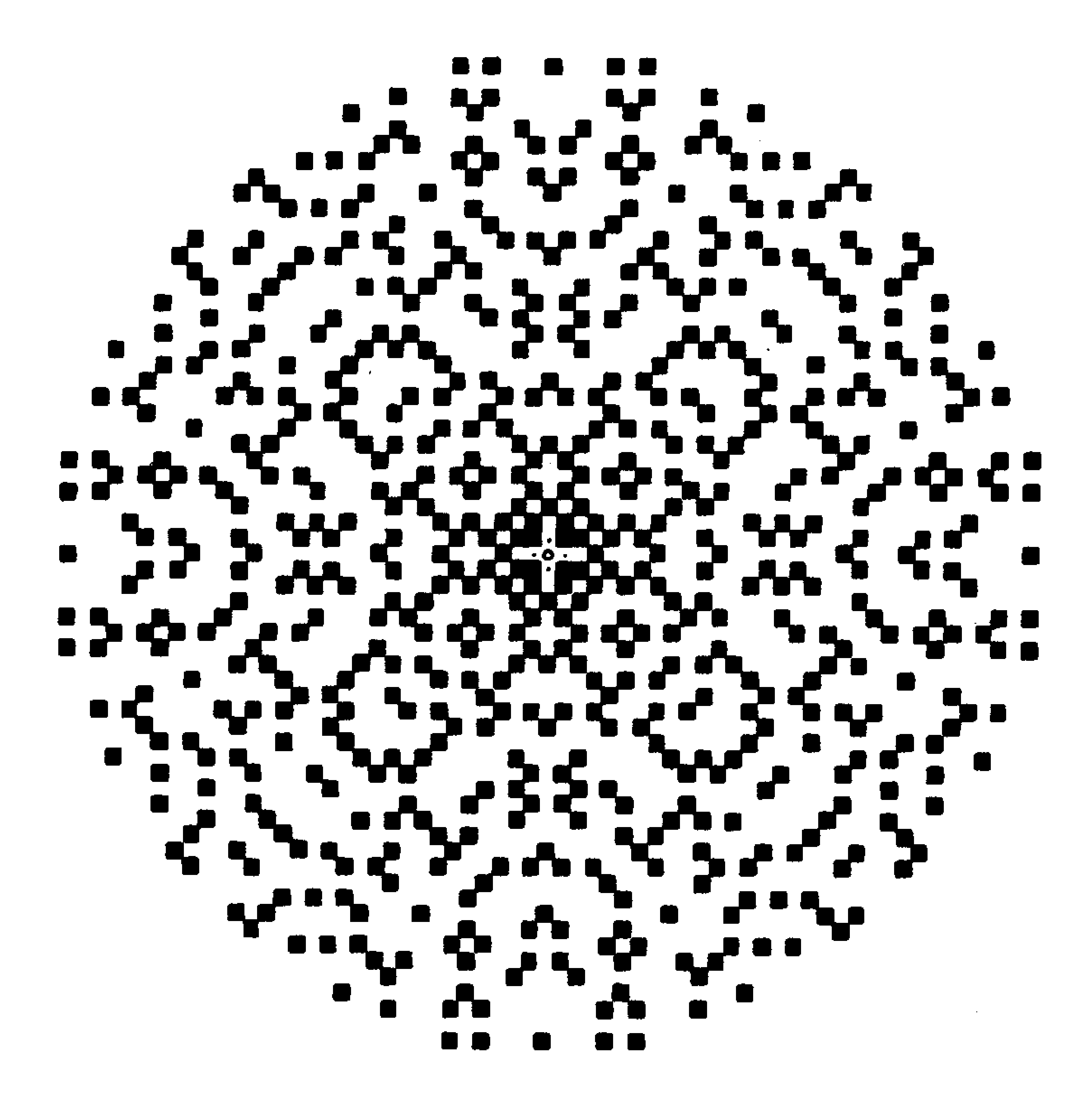


图 4　范数小于 1000 的 Gauss 素数

很有意思的图案(图 4). 它被用来作地砖及桌布.

Motzkin 和 Gordon 问道:以 Gauss 素数作为踏脚石,取长为有界的步子,是否可以从原点"走"到无穷远呢? 猜测是不行的. Jordan 和 Rabung 指出:步长至少为 4 是必要的.

Eisenstein-Jacobi 整数(Eisenstein-Jacobi integer) $a+b\omega$(其中 a, b 是整数, ω 是一个复的三次单位根,满足 $\omega^2+\omega+1=0$)也有惟一分解,其中的素数再次构成一个图案(图 5),这一次图案有六边形的对称,因为它有六个单位 $\pm 1, \pm \omega, \pm \omega^2$. 素数 2 和形如 $6k-1$ 的素数(5, 11, 17, 23, 29, 41, …)仍为 Eisenstein-Jacobi 素数,但是 3 和那些形如 $6k+1$ 的素数则可以分解:

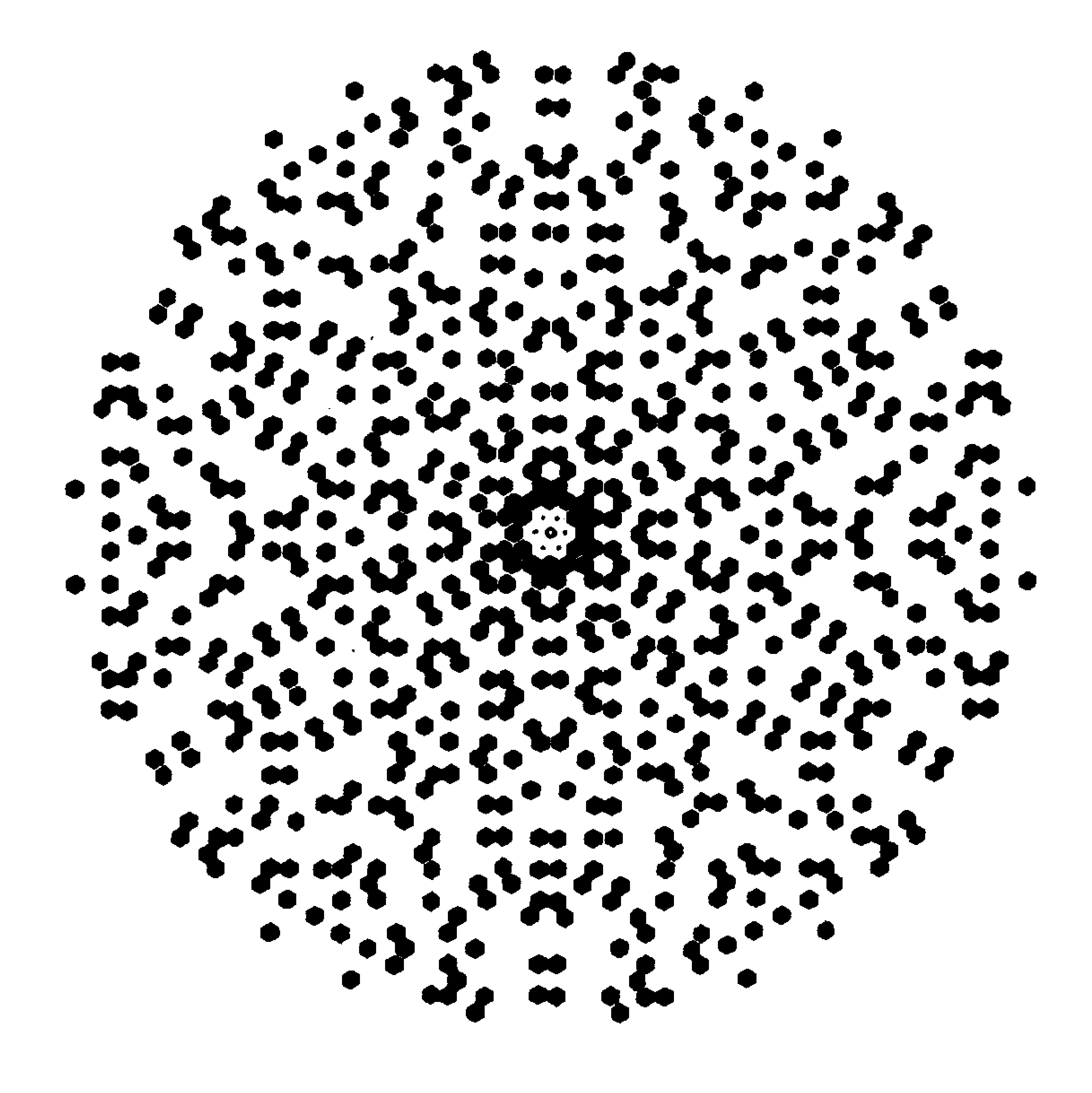


图 5　Eisenstein-Jacobi 素数

$3=(1-\omega)(1-\omega^2)$, $7=(2-\omega)(2-\omega^2)$, $13=(3-\omega)(3-\omega^2)$, $19=(3-2\omega)(3-2\omega^2)$, $31=(5-\omega)(5-\omega^2)$, $37=(4-3\omega)(4-3\omega^2)$, $\cdots$.

John Leech 希望找到由 Gauss 素数以及由 Eisenstein-Jacobi 素数组成的长算术级数. 在图 4 中他找到 9 个,在图 5 中找到 12 个. 后来他发现了由 10 个 Gauss 素数组成的算术级数

$$-8-13i,\quad -3-8i,\quad 2-3i,\quad 7+2i,\quad \cdots,\quad 37+32i,$$

其中最后 3 个在图 4 以外.

参考文献

J. H. Jordan & J. R. Rabung, A conjecture of Paul Erdős concerning Gaussian primes, *Math. Comput.*, **24**(1970) 221-223.

A17. 素数公式

数论的酵母似乎是 p_n 的公式,或是 $\pi(x)$的公式,或者是判断素性的充分必要条件. Wilson 定理似乎是独一无二的 (Vantieghem 的结果: $p>2$ 是素数,当且仅当 $\prod_{d=1}^{p-1}(2^d-1)\equiv p \bmod 2^p-1$ 是否与之等价?);但即使是 Wilson 定理对计算也没有用. C. W. Williams 和 C. P. Wormel 用它给出一个只用到初等函数的公式,但该公式过于复杂,无法放在这里. Mann-Shanks 算法是又一个难得的东西,但很少有实用价值. Matiyasevich 和其他的逻辑学者利用 Wilson 定理以及他们有关 Hilbert 第十问题的解造出了一种多项式,这种多项式的值域的正的部分恰好是素数集.

Boris Stechkin 的三个定理值得提及. 它们基于函数

$$S(n)=\#\left\{m: 2\leqslant m\leqslant n, (m-1)\left|\left\lfloor\frac{n(m-1)}{m}\right\rfloor\right.\right\}.$$

(1) $n-1$ 为素数仅当 $S(n)=d(n)$,这里 $d(n)$表示 n 的因子个数.

(2) $n\pm1$ 为孪生素数仅当 $S(n)+S(n+1)=2d(n)$.

(3) $p<q$(奇素数)蕴含 $S(q)-S(q-1)+S(q-2)-\cdots-S(p+1)=0$.

有关这个论题有大量的论文,其复杂性及目的不尽相同.看来值得对下列各问题加以区分:

1. 作为 x 的函数的 $\pi(x)$ 的公式.
2. 作为 n 的函数的 p_n 的公式.
3. n 为素数的充分必要条件.
4. 对定义域中每个元素都取素数值的函数.
5. 一个函数,它的值域的正值仅由素数组成,或由全体素数组成.
6. 一个其值域包含高密度素数集合的函数.
7. 表示 n 的最大素因子的公式.
8. 表示 n 的素因子的公式.
9. 表示大于 n 的最小素数的公式.
10. 用 $p_1,p_2,\cdots,p_n$ 表示 p_{n+1} 的公式.
11. 生成素数的算法,等等.

每一个问题的例子都可以在文献中找到.(在 A1 中)我们已经提到 Euler 的著名公式 n^2+n+41.在某种意义上说它是最好可能的,不过用判别式为正数的二次表达式甚至可以产生更长的一列素数值(虽然其中有一些可能是负的).Gilbert Fung 给出表达式 $47n^2-1701n+10181$,它对 $0\leqslant n\leqslant 42$ 取素数值,其判别式为 $\Delta=979373$;而 Russell Ruby 则给出 $36n^2-810n+2753, 0\leqslant n\leqslant 44, \Delta=2^2\cdot 3^2\cdot 7213$.

Euler 公式的前 1000 个值中有 581 个素数.Edgar Karst 在他 1991 年 1 月 1 日的一封信中用 $2n^2-199$ 的 598 个素数值打破了这一记录.Stsphen Williams 宣布得到 $2n^2-1000n-2609$ 的 602 个素数值.他们的公式在前 10000 个数中对应取到的素数个数分别为 4148、4373 和 4151 个.然而,有意义的并不是经过前面如此多的数的实际的密度(显然在所有情形其密度均趋于 0),而是它的渐近(asymptotic)密度.如果我们永远相信 Hardy 和 Littlewood

的话(见 A1),此渐近密度恒为 $c\sqrt{n}/\ln n$,我们能做的最好的事就是让 c 的值尽可能地大. 对于 Beeger 给出的多项式 $x^2+x+27941$, Shanks 算出有 $c=3.6319998$. Funf 和 Williams 对多项式 $x^2+x+132874279528931$ 算出有 $c=5.0870883$. 若 Δ 是二次多项式的判别式,那么 Legendre 符号 $\left(\frac{\Delta}{p}\right)$(见 F5)对很少的小素数 p 取值为 1.

Sierpiński 注意到由 Fermat 定理可得:若 n 为素数,则 n 整除

$$1^{n-2}+2^{n-1}+\cdots+(n-1)^{n-1}+1.$$

其逆是否为真? Giuga 猜想这是对的,并对 $n\leqslant 10^{1000}$ 作了验证,而 Bedocchi 则对 $n\leqslant 10^{1700}$ 作了验证. Giuga 注意到其反例应是一个 Carmichael 数(A12,A13),又 $p\mid n$ 将蕴含 $(p-1)\mid(n-1)$ 且

$$\sum_{p\mid n}\frac{1}{p}-\frac{1}{n}$$

必为整数,从而 n 至少有 8 个不同的素因子. 一个等价的猜想是

$$nB_{n-1}\equiv -1 \mod n,$$

其中 Bernoulli 数 (Bernoulli number) B_k 是 $x/(e^x-1)=\sum_{k\geqslant 0}B_kx^k/k!$ 的展开式中的系数(与 D2 比较).

参考文献

Ulrich Abel & Hartmut Siebert, Sequences with large numbers of prime values, *Amer. Math. Monthly*, **100**(1993) 167–169.

William W. Adams, Eric Liverance & Daniel Shanks, Infinitely many necessary and sufficient conditions for primality, *Bull. Inst. Combin. Appl.*, **3**(1991) 69–76; *MR* **90e**:11011.

A. R. Ansari, On prime representing function, *Ganita*, **2**(1951) 81–82; *MR* **15**, 11.

Thøger Bang, A function representing all prime numbers, *Norsk Mat. Tidsskr.*, **34**(1952) 117–118; *MR* **14**, 621.

V. I. Baranov & B. S. Stechkin, *Extremal Combinatorial Problems and their Applications*, Kluwer, 1993, Problem 2.22.

Paul T. Bateman & Roger A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comput.*, **16**(1962) 363–367.

Christoph Baxa, Über Gandhis Primzahlformel, *Elem. Math.*, **47**(1992) 82–84; *MR* **93h**: 11007.

E. Bedocchi, Nota ad una congettura sui numeri primi, *Riv. Mat. Univ. Parma*(4), **11**(1985) 229–236.
J. Braun, Das Fortschreitungsgesetz der Primzahlen durch eine transcendente Gleichung exakt dargestelt, *Wiss. Beilage Jahresber. Fr. W. Gymn. Trier*, 1899, 96 pp.
R. Creighton Buck, Prime representing functions, *Amer. Math. Monthly*, **53**(1946) 265.
John H. Conway, Problem 2.4, *Math. Intelligencer*, **3**(1980) 45.
L. E. Dickson, *History of the Theory of Numbers*, Carnegie Institute, Washington, 1919, 1920, 1923; reprinted Stechert, New York, 1934; Chelsea, New York, 1952, 1966, Vol. I, Chap. XVIII.
Underwood Dudley, History of a formula for primes, *Amer. Math. Monthly*, **76**(1969) 23–28; *MR* **38** #4270.
Underwood Dudley, Formulas for primes, *Math. Mag.*, **56**(1983) 17–22.
D. D. Elliott, A prime generating function, *Two-Year Coll. Math. J.*, **14**(1983) 57.
David Ellis, Some consequences of Wilson's theorem, *Univ. Nac. Tucumán Rev. Ser. A*, **12**(1959) 27–29; *MR* **21** #7179.
Reijo Ernvall, A formula for the least prime greater than a given integer, *Elem. Math.*, **30**(1975) 13–14; *MR* **54** #12616.
Robin Forman, Sequences with many primes, *Amer. Math. Monthly*, **99**(1992) 548–557; *MR* **93e**:11104.
Gilbert W. Fung & Hugh Cowie Williams, Quadratic polynomials which have a high density of prime values, *Math. Comput.* (199).
J. M. Gandhi, Formulae for the n-th prime, *Proc. Washington State Univ. Conf. Number Theory*, Pullman, 1971, 96–106; *MR* **48** #218.
Betty Garrison, Polynomials with large numbers of prime values, *Amer. Math. Monthly*, **97**(1990) 316–317; *MR* **91i**:11124.
Giuseppe Giuga, Sopra alcune proprietà caratteristiche dei numeri primi, *Period. Math.* (4), **23**(1943) 12–27; *MR* **8**, 11.
Giuseppe Giuga, Su una presumibile proprietà caratteristica dei numeri primi, *Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat.*(3), **14(83)**(1950) 511–528; *MR* **13**, 725.
P. Goetgheluck, On cubic polynomials giving many primes, *Elem. Math.*, **44**(1989) 70–73; *MR* **90j**:11014.
Solomon W. Golomb, A direct interpretation of Gandhi's formula, *Amer. Math. Monthly*, **81**(1974) 752–754; *MR* **50** #7003.
Solomon W. Golomb, Formulas for the next prime, *Pacific J. Math.*, **63**(1976) 401–404; *MR* **53** #13094.
R. L. Goodstein, Formulae for primes, *Math. Gaz.*, **51**(1967) 35–36.
H. W. Gould, A new primality criterion of Mann and Shanks, *Fibonacci Quart.*, **10**(1972) 355–364, 372; *MR* **47** #119.
Richard K. Guy, Conway's prime producing machine, *Math. Mag.*, **56**(1983) 26–33; *MR* **84j**:10008.
G. H. Hardy, A formula for the prime factors of any number, *Messenger of Math.*, **35**(1906) 145–146.

V. C. Harris, A test for primality, *Nordisk Mat. Tidskr.*, **17**(1969) 82; *MR* **40** #4197.

E. Härtter, Über die Verallgemeinerung eines Satzes von Sierpiński, *Elem. Math.*, **16** (1961) 123–127; *MR* **24** #A1869.

Olga Higgins, Another long string of primes, *J. Recreational Math.*, **14** (1981/82) 185.

C. Isenkrahe, Ueber eine Lösung der Aufgabe, jede Primzahl als Function der vorhergehenden Primzahlen durch einen geschlossenen Ausdruck darzustellen, *Math. Ann.*, **53**(1900) 42–44.

James P. Jones, Formula for the n-th prime number, *Canad. Math. Bull.*, **18** (1975) 433–434; *MR* **57** #9641.

James P. Jones, Daihachiro Sato, Hideo Wada & Douglas Wiens, Diophantine representation of the set of prime numbers, *Amer. Math. Monthly*, **83**(1976) 449–464; *MR* **54** #2615.

James P. Jones & Yuri V. Matiyasevich, Proof of recursive unsolvability of Hilbert's tenth problem, *Amer. Math. Monthly*, **98**(1991) 689–709; *MR* **92i**:03050.

Steven Kahan, On the smallest prime greater than a given positive integer, *Math. Mag.*, **47**(1974) 91–93; *MR* **48** #10964.

E. Karst, The congruence $2^{p-1} \equiv 1 \bmod p^2$ and quadratic forms with a high density of primes, *Elem. Math.*, **22**(1967) 85–88.

John Knopfmacher, Recursive formulae for prime numbers, *Arch. Math. (Basel)*, **33** (1979/80) 144–149; *MR* **81j**:10008.

Masaki Kobayashi, Prime producing quadratic polynomials and class-number one problem for real quadratic fields, *Proc. Japan Acad. Ser. A Math. Sci.*, **66**(1990) 119–121; *MR* **91i**:11140.

L. Kuipers, Prime-representing functions, *Nederl. Akad. Wetensch. Proc.*, **53** (1950) 309–310 = *Indagationes Math.*, **12**(1950) 57–58; *MR* **11**, 644.

J. C. Lagarias, V. S. Miller & A. M. Odlyzko, Computing $\pi(x)$: the Meissel-Lehmer method, *Math. Comput.*, **44**(1985) 537–560.

Klaus Langmann, Eine Formel für die Anzahl der Primzahlen, *Arch. Math. (Basel)*, **25**(1974) 40; *MR* **49** #4951.

D. H. Lehmer, On the function x^2+x+A, *Sphinx*, **6**(1936) 212–214; **7**(1937) 40.

S. Louboutin, R. A.Mollin & H. C. Williams, Class numbers of real quadratic fields, continued fractions, reduced ideals, prime-producing polynomials and quadratic residue covers, *Canad. J. Math.*, **44**(1992) 1–19.

H. B. Mann & Daniel Shanks, A necessary and sufficient condition for primality and its source, *J. Combin. Theory Ser. A*, **13**(1972) 131–134; *MR* **46** #5225.

J.-P. Massias & G. Robin, Effective bounds for some functions involving prime numbers, Preprint, Laboratoire de Théorie des Nombres et Algorithmique, 123 rue A. Thomas, 87060 Limoges Cedex, France.

Yuri V. Matiyasevich, Primes are enumerated by a polynomial in 10 variables, *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov*,**68**(1977) 62–82, 144–145; *MR* **58** #21534; English translation: *J. Soviet Math.*, **15**(1981) 33–44.

W. H. Mills, A prime-representing function, *Bull. Amer. Math. Soc.*, **53**(1947) 604; *MR* **8**, 567.

Richard A. Mollin, Prime valued polynomials and class numbers of quadratic fields, *Internat. J. Math. Math. Sci.*, **13**(1990) 1–11; *MR* **91c**:11060.

Richard A. Mollin, Ambiguous classes in quadratic fields, *Math. Comput.*, **61** (1993) 355–360.

Richard A. Mollin & Hugh Cowie Williams, Quadratic nonresidues and prime-producing polynomials, *Canad. Math. Bull.*, **32**(1989) 474–478; *MR* **91a**:11009. [see also *Number Theory*, de Gruyter, 1989, 654–663 and *Nagoya Math. J.*, **112**(1988) 143–151.]

Leo Moser, A prime-representing function, *Math. Mag.*, **23**(1950) 163–164.

K. S. Namboodiripad, A note on formulae for the n-th prime, *Monatsh. Math.*, **75**(1971) 256–262; *MR* **46** #126.

T. B. M. Neill & M. Singer, The formula for the Nth prime, *Math. Gaz.*, **49**(1965) 303.

Ivan Niven, Functions which represent prime numbers, *Proc. Amer. Math. Soc.*, **2**(1951) 753–755; *MR* **13**, 321a.

O. Ore, On the selection of subsequences, *Proc. Amer. Math. Soc.*, **3**(1952) 706–712; *MR* **14**, 256.

Joaquin Ortega Costa, The explicit formula for the prime number function $\pi(x)$, *Revista Mat. Hisp.-Amer.*(4), **10**(1950) 72–76; *MR* **12**, 392b.

Makis Papadimitriou, A recursion formula for the sequence of odd primes, *Amer. Math. Monthly*, **82**(1975) 289; *MR* **52** #246.

Carlos Raitzin, The exact count of the prime numbers that do not exceed a given upper bound (Spanish), *Rev. Ingr.*, **1**(1979) 37–43; *MR* **82e**:10074.

Stephen Regimbal, An explicit formula for the k-th prime number, *Math. Mag.*, **48**(1975) 230–232; *MR* **51** #12676.

J. B. Rosser & L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, **6**(1962) 64–94.

Michael Rubinstein, A formula and a proof of the infinitude of the primes, *Amer. Math. Monthly*, **100**(1993) 388–392.

W. Sierpiński, *Elementary Number Theory*, (ed. A. Schinzel) PWN, Warszawa, 1987, p. 218.

W. Sierpiński, Sur une formule donnant tous les nombres premiers, *C.R. Acad. Sci. Paris*, **235**(1952) 1078–1079; *MR* **14**, 355.

W. Sierpiński, Les binômes $x^2 + n$ et les nombres premiers, *Bull. Soc. Royale Sciences Liège*, **33**(1964) 259–260.

B. R. Srinivasan, Formulae for the n-th prime, *J. Indian Math. Soc. (N.S.)*, **25**(1961) 33–39; *MR* **26** #1289.

B. R. Srinivasan, An arithmetical function and an associated formula for the n-th prime. I, *Norske Vid. Selsk. Forh. (Trondheim)*, **35**(1962) 68–71; *MR* **27** #101.

Garry J. Tee, Simple analytic expressions for primes, and for prime pairs, *New Zealand Math. Mag.*, **9**(1972) 32–44; *MR* **45** #8601.

E. Teuffel, Eine Rekursionsformel für Primzahlen, *Jber. Deutsch. Math Verein.*, **57**(1954) 34–36; *MR* **15**, 685.

John Thompson, A method for finding primes, *Amer. Math. Monthly*, **60** (1953) 175; *MR* **14**, 621.

P. G. Tsangaris & James P. Jones, An old theorem on the GCD and its application

to primes, *Fibonacci Quart.*, **30**(1992) 194–198; *MR* **93e**:11004.

Charles Vanden Eynden, A proof of Gandhi's formula for the n-th prime, *Amer. Math. Monthly*, **79**(1972) 625; *MR* **46** #3425.

E. Vantieghem, On a congruence only holding for primes, *Indag. Math.(N.S.)*, **2**(1991) 253–255; *MR* **92e**:11005.

C. P. Willans, On formulae for the Nth prime number, *Math. Gaz.*, **48**(1964) 413–415.

C. P. Wormell, Formulae for primes, *Math. Gaz.*, **51**(1967) 36–38.

E. M. Wright, A prime representing function, *Amer. Math. Monthly*, **58**(1951) 616–618; *MR* **13**, 321b.

E. M. Wright, A class of representing functions, *J. London Math. Soc.*, **29** (1954) 63–71; *MR* **15**, 288d.

A18. Erdös-Selfridge 的素数分类法

Erdös和 Selfridge 对素数作了如下分类：p 在类 1 中，如果 $p+1$的仅有的素因子是 2 或 3；p 在类 r 中，如果 $p+1$ 的每个素因子都在它前面 $r-1$ 个类的某类中，且至少有一个素因子在类 $r-1$ 中.例如：

类 1：2 3 5 7 11 17 23 31 47 53 71 107 127 191 431 647 863 971…

类 2：13 19 29 41 43 59 61 67 79 83 89 97 101 109 131 137 139 149 167 179 197 199 211 223 229 239 241 251 263 269 271 281 283 293 307 317 319 359 367 373 377 383 419 439 449 461 467 499 503 509 557 563 577 587 593 599 619 641 643 659 709 719 743 751 761 769 809 827 839 881 919 929 953 967 979 991 1019…

类 3：37 103 113 151 157 163 173 181 193 227 233 257 277 311 331 337 347 353 379 389 397 401 409 421 457 463 467 487 491 521 523 541 547 571 601 607 613 631 653 683 701 727 733 773 787 811 821 829 853 857 859 877 883 911 937 947 983 997 1009 1013 1021…

类 4：73 313 443 617 661 673 677 691 739 757 823 887 907 941 977…

类 5：1321，1381…

容易证明，对任何 $\varepsilon>0$ 和所有 r，类 r 中不超过 n 的素数个数为 $o(n^{\varepsilon})$. 证明在每个类中有无穷多个素数. 若用 $p_1^{(r)}$ 记类 r 中的最小素数，则 $p_1^{(1)}=2$，$p_1^{(2)}=13$，$p_1^{(3)}=37$，$p_1^{(4)}=73$，$p_1^{(5)}=1021$，Erdös 认为有 $(p_1^{(r)})^{1/r}\to\infty$，而 Selfridge 则认为它像是有界的.

如果用 $p-1$ 代替 $p+1$，就给出一个类似的分类法：

类 1：2 3 5 7 13 17 19 37 73 97 109 163 193 433 487 577 769 1153 …

类 2：11 29 31 41 43 53 61 71 79 101 103 113 127 131 137 149 151 157 181 191 197 211 223 229 239 241 251 257 271 281 293 307 313 337 379 389 401 409 421 439 443 449 459 491 521 541 547 571 593 601 613 631 641 647 653 673 677 701 751 757 761 773 811 877 883 911 919 937 953 971 1009 1021…

类 3：23 59 67 83 89 107 173 199 227 233 263 311 317 331 349 353 367 373 383 397 419 431 463 479 503 509 523 563 569 587 607 617 619 661 683 727 733 739 743 787 809 821 823 853 859 881 887 907 929 947 977 983 991 1031 1033…

类 4：47 139 167 179 269 277 347 461 467 499 599 643 691 709 797 827 829 839 857 863 967 997 1013 1019…

类 5：283 359 557 659 941…

类 6：719 1319…

类 7：1439…

对此分类预料会有类似的答案. 对应的类是否密度相等？它和 Cunningham 链(A7)有联系.

参考文献

P. Erdős, Problems in number theory and combinatorics, *Congr. Numer. XVIII*, Proc. 6th Conf. Numer. Math., Manitoba, 1976, 35–58 (esp. p. 53); *MR* **80e**:10005.

A19. 使 $n-2^k$ 取素数值的 n,形状不是 $\pm p^a \pm 2^b$ 的奇素数

Erdös 猜想:对所有满足 $2 \leqslant 2^k < n$ 的 k,使 $n-2^k$ 取素数值的 n 仅有 4,7,15,21,45,75 和 105. Mientka 和 Weitzenkamp 对 $n < 2^{44}$作了验证,Uchiyama 和 Yorinaga 验证到 2^{77}. Vaughan 证明了这种数不太多,在小于 x 的范围内其个数少于 $x\exp\{-(\ln x)^c\}$,但他没能证明其个数少于 $x^{1-\varepsilon}$.

Erdös 又猜想对无穷多个 n,所有整数 $n-2^k(1 \leqslant 2^k < n)$都是无平方因子数(也见 F13).

如果用 $A(x)$记不超过 x 且使 $n-2^k(2 \leqslant 2^k < n)$为素数的整数 n 的个数,则 Hooley 证明了:广义 Riemann 猜想蕴含 $A(x)= O(x^c)$($c<1$ 为显常数),Narkiewicz 将它改进为 $c<\frac{1}{2}$.

Cohen 和 Selfridge 希望求出形状不是 $\pm p^a \pm 2^b$ 的最小正奇数,其中 p 是素数,$a \geqslant 0, b \geqslant 1$,正负号可任取. 他们注意到此数大于 2^{18},但至多

6120 6699060672 7677809211 5601756625 4819576161-
6319229817 3436854933 4512406741 7420946855 8999326569.

Crocker 证明了有无穷多个形状不是 2^k+2^l+p 的奇整数,这里 p 为素数. Erdös 认为在小于 x 的整数中可能有 cx 个这样的数,但能否证明有 $> x^{\varepsilon}$ 个呢? 我们可否证明在这里覆盖同余系(F13)没有助益呢? 也即,是否 $p+2^u+2^v$(或 $p+2^u+2^v+2^w$)满足每个算术级数? 更一般地,Erdös 问道:对每个 r,是否存在无穷多个奇整数,它们都不是一个素数加上 2 的不超过 r 次幂的和? 它们的密度是否都是正数? 它们包含一个无限的算术级数吗? 在相反的方向上,Gallagher 证明了:对每个 $\varepsilon>0$,存在一个充分大的 r,使素数加上 2 的 r 次幂的和组成的序列之下密度大于 $1-\varepsilon$.

Erdös 还问道:是否有形状不是 2^k+s 的奇整数? 这里 s 为无

平方因子数.

设 $f(n)$ 为 n 表示为和式 2^k+p 的表法数，$\{a_i\}$ 为使 $f(n)>0$ 的 n 的值的序列. $\{a_i\}$ 的密度是否存在? Erdös 证明了无穷多次有 $f(n)>c\ln\ln n$，但不能确定是否有 $f(n)=o(\ln n)$. 他猜想有 $\limsup(a_{i+1}-a_i)=\infty$. 如果对任意大的最小模有覆盖同余系，则可推出此猜想为真.

Carl Pomerance 注意到，对 $n=210$，则对满足 $n/2<p<n$ 的所有 p，$n-p$ 皆为素数，他问是否存在任何其他像这样的 n? 由于 Deshouillers 的帮助，Granville 和 Narkiewicz 后来对此问题给出了否定的回答.

参考文献

Fred Cohen & J. L. Selfridge, Not every number is the sum or difference of two prime powers, *Math. Comput.*, **29**(1975) 79–81; *MR* **51** #12758.

R. Crocker, On the sum of a prime and of two powers of two, *Pacific J. Math.*, **36**(1971) 103–107; *MR* **43** #3200.

Jean-Marc Deshouillers, Andrew Granville, Władysław Narkiewicz & Carl Pomerance, An upper bound in Goldbach's problem, *Math. Comput.*, **61**(1993) 209–213.

P. Erdős, On integers of the form 2^r+p and some related problems, *Summa Brasil. Math.*, **2**(1947-51) 113–123; *MR* **13**, 437.

Patrick X. Gallagher, Primes and powers of 2, *Inventiones Math.*, **29**(1975) 125–142; *MR* **52** #315.

C. Hooley, *Applications of Sieve Methods*, Academic Press, 1974, Chap. VIII.

Donald E. G. Malm, A graph of primes, *Math. Mag.*, **66**(1993) 317–320.

Walter E. Mientka & Roger C. Weitzenkamp, On f-plentiful numbers, *J. Combin. Theory*, **7**(1969) 374–377; *MR* **42** #3015.

W. Narkiewicz, On a conjecture of Erdős, *Colloq. Math.*, **37**(1977) 313–315; *MR* **58** #21971.

A. de Polignac, Recherches nouvelles sur les nombres premiers, *C. R. Acad. Sci. Paris*, **29**(1849) 397–401, 738–739.

Saburô Uchiyama & Masataka Yorinaga, Notes on a conjecture of P. Erdős, I, II, *Math. J. Okayama Univ.*, **19**(1977) 129–140; **20**(1978) 41–49; *MR* **56** #11929; **58** #570.

R. C. Vaughan, Some applications of Montgomery's sieve, *J. Number Theory*, **5**(1973) 64–79; *MR* **49** #7222.

B. 整 除 性

我们将用 $d(n)$ 记 n 的正因子的个数，用 $\sigma(n)$ 记 n 的正因子之和，用 $\sigma_k(n)$ 记 n 的正因子的 k 次幂之和，于是有 $\sigma_0(n)=d(n)$ 及 $\sigma_1(n)=\sigma(n)$. 用 $s(n)$ 表示 n 的**真因子**(aliquot part)之和，即除去 n 自身以外的所有其他的正因子之和，于是有 $s(n)=\sigma(n)-n$. n 的不同素因子的个数记为 $\omega(n)$，而 n 的所有素因子的个数(按重数计算)记为 $\Omega(n)$.

各种算术函数的迭代将用统一的方式来记，例如 $s^k(n)$ 定义如下：$s^0(n)=n, s^{k+1}(n)=s(s^k(n))$(对 $k\geqslant 0$).

我们用记号 $d\mid n$ 表示 d 整除 n，$e\nmid n$ 表示 e 不整除 n. 记号 $p^k\parallel n$ 表示 $p^k\mid n$ 但 $p^{k+1}\nmid n$. 记号 $[m,n]$ 表示连续整数 $m, m+1, \cdots, n$.

B1. 完 全 数

完全数(perfect number)是满足 $s(n)=n$ 的数. Euclid 已经知道：如果 2^p-1 是素数，则 $2^{p-1}(2^p-1)$ 是一个完全数，例如 6，28，496，…，见 A3 中的 Mersenne 素数表. Euler 证明了：这些是仅有的偶完全数.

是否存在奇完全数更是数论中一个尽人皆知的没有解决的问题. 奇完全数的下界已被 Brent，Cohen 及 te Riele 等人提升到 10^{300}. Brandstein 证明了奇完全数的最大素因子 >500000，而 Hagis 则证明了奇完全数的第二大素因子 >1000. Cohen 证明了奇完全数包含一个 $>10^{20}$ 的素数幂因子，而 Sayers 则证明了奇完全数至少有 29 个(不一定不相同的)素因子.

Pomerance 证明了：有至多 k 个不同素因子的奇完全数小于

$$(4k)^{(4k)^{2^{k^2}}}.$$

而 Heath-Brown 对此作了很大改进,他证明了:如果 n 为一个奇数且满足 $\sigma(n)=an$,那么 $n<(4d)^{4^k}$,这里 d 是 a 的分母,k 是 n 的不同素因子的个数.特别地,如果 n 是一个有 k 个不同素因子的奇完全数,则 $n<4^{4^k}$.

John Leech 希望找到像 Descartes 给出的数

$$3^2 7^2 11^2 13^2 22021$$

那样的假奇完全数,如果假意把 22021 当做是素数的话,那么该数就是一个奇完全数.

关于许多较早的文献,请见本书第一版.

参考文献

Michael S. Brandstein, New lower bound for a factor of an odd perfect number, #82T-10-240, *Abstracts Amer. Math. Soc.*, **3**(1982) 257.

Richard P. Brent & Graeme L. Cohen, A new lower bound for odd perfect numbers, *Math. Comput.*, **53**(1989) 431–437.

R. P. Brent, G. L. Cohen & H. J. J. te Riele, Improved techniques for lower bounds for odd perfect numbers, *Math. Comput.*, **57**(1991) 857-868; *MR* **92c**:11004.

Graeme L. Cohen, On the largest component of an odd perfect number, *J. Austral. Math. Soc. Ser. A*, **42**(1987) 280–286.

P. Hagis, Sketch of a proof that an odd perfect number relatively prime to 3 has at least eleven prime factors, *Math. Comput.*, **40**(1983) 399–404.

P. Hagis, On the second largest prime divisor of an odd perfect number, *Lecture Notes in Math.*, **899**, Springer-Verlag, New York, 1971, pp. 254–263.

D. R. Heath-Brown, Odd perfect numbers, (submitted).

Masao Kishore, Odd perfect numbers not divisible by 3 are divisible by at least ten distinct primes, *Math. Comput.*, **31**(1977) 274–279; *MR* **55** #2727.

Masao Kishore, Odd perfect numbers not divisible by 3. II, *Math. Comput.*, **40**(1983) 405–411.

M. D. Sayers, An improved lower bound for the total number of prime factors of an odd perfect number, M.App.Sc. Thesis, NSW Inst. Tech., 1986.

B2. 殆完全数，拟完全数，伪完全数，调和数，奇异数，重完全数和超完全数

似乎由于在推翻奇完全数存在性这一问题上屡战屡败，挫折惨重，众多著者转而定义了许多与之密切相关的概念，提出了大量的问题，其中许多问题看起来比原来的问题更容易处理.

对一个完全数有 $\sigma(n)=2n$. 若 $\sigma(n)<2n$，它就叫做亏数(deficient). 在 *Abacus* 一书中有一个问题就是证明：要么每个数 $n>3$ 都是两个亏数之和，或者找出一个无此性质的数. 若 $\sigma(n)>2n$，称之为过剩数(abundant). 如果 $\sigma(n)=2n-1$，则 n 称为殆完全数(almost perfect). 2 的幂是殆完全数；但不知道是否还有任何别的数也是殆完全数. 如果 $\sigma(n)=2n+1$，则 n 称为拟完全数(quasi-perfect). 拟完全数必为奇平方数，然而无人知道是否有这样的数存在. Masao Kishore 指出：若 n 是一个拟完全数，则 $n>10^{30}$ 且 $\omega(n)\geqslant 6$. Hagis 和 Cohen 将此结果改进为 $n>10^{35}$ 且 $\omega(n)\geqslant 7$. Cattaneo 原来曾经宣布他证明了 $3\nmid n$，但是 Sierpiński 和其他人注意到他的证明有误. Kravitz 在一封信中做出一个更一般的猜想：不存在这样的数，它的过剩量(abundance)(即 $\sigma(n)-2n$)是一个奇平方数. 有关这一点 Graeme Cohen 写道：有趣的是

$$\sigma(2^2 3^2 5^2) = 3(2^2 3^2 5^2) + 11^2,$$

又若有 $\sigma(n)=2n+k^2$ 及 $n\perp k$，那么 $\omega(n)\geqslant 4$ 且 $n>10^{20}$. 他还证明了：如果 $k<10^{10}$，则 $\omega(n)\geqslant 6$；若 $k<44366047$，则 n 是一个本原的过剩数(见下述). 后来将条件 $n\perp k$ 放宽，他找到了解

$$n = 2\cdot 3^2\cdot 238897,\quad k = 3^2\cdot 23\cdot 1999$$

和 5 个解 $n=2^2\cdot 7^2\cdot p^2$，其中

$p=$	53	277	541	153941	358276277
$k=$	$7\cdot 29$	$5\cdot 7\cdot 23$	$5\cdot 7\cdot 43$	$5\cdot 7\cdot 103\cdot 113$	$5\cdot 7\cdot 227\cdot 29\cdot 521$.

他验证出后 5 个中的第一个是有奇的平方过剩量的最小整数. 在那以后 Sidney Kravitz 又给出两个解

$$n=2^3\cdot 3^2\cdot 1657^2,\qquad k=3\cdot 11\cdot 359,$$

$$n=2^4\cdot 31^2\cdot 7992220179128893^2,\qquad k=44498798693247589.$$

在后一解中有 31 整除 k. Erdös 想求刻画使 $|\sigma(n)-2n|<C$(对某个常数 C)成立的大数之特征. 例如 $n=2^m$: 对其他的无穷多个类,见 Mąkowski 的两篇论文.

Wall, Crews 和 Johson 证明了:过剩数的密度在 0.2441 和 0.2909之间. 在1983 年8 月 17 日的一封信中,Wall 断言把上述范围缩小到了 0.24750 和0.24893 之间. Erdös 问这一密度是否是无理数?

Sierpiński 称一个数为伪完全数(pseudoperfect),如果它是它的某些因子的和. 例如 20 = 1 + 4 + 5 + 10. Erdös 证明了它们的密度存在,又说或许存在整数 n,它不是伪完全数,但有 $n=ab$, a 为过剩数,而 b 有许多素因子:实际上 b 能有许多小于 a 的素因子吗?

对 $n\geqslant 3$, Abbott 用 $l=l(n)$表示满足下列条件的最小整数:存在 n 个整数 $1\leqslant a_1<a_2<\cdots<a_n=l$,使得对每个 i 有 $a_i\mid s=\sum a_i$ (于是 s 是伪完全数). 他能证明:对某个 $c_1>0$ 和所有 $n\geqslant 3$ 有 $l(n)>n^{c_1\ln\ln n}$,又对某个 $c_2>0$ 和无穷多个 n 有 $l(n)<n^{c_2\ln\ln n}$.

称一个数为本原过剩(primitive abundant)的,如果它是过剩数,但它所有的真因子都是亏数. 称一个数为本原伪完全数(primitive pseudoperfect),如果它是伪完全数,但它所有的真因子都不是伪完全数. 如果 n 的所有因子的调和平均是一个整数, Pomerance 称之为一个调和数(harmonic number). A. Zachariou 和 E. Zachariou 称这些数为"Ore 数",称本原伪完全数为"不可约半完全数". 他们注意到伪完全数的任何倍数都是伪完全数,伪完全数与调和数都把完全数作为它们的真子集. 最后这个结果属于 Ore. 所有的数 $2^m p$($m\geqslant 1$, p 是在 2^m 和 2^{m+1}之间的素数)都是本原伪完全数,但也有不是此形状的本原伪完全数,如 770. 有无穷多个不

是调和数的本原伪完全数. 最小的奇本原伪完全数是 945. Erdös 能证明奇本原伪完全数个数无穷.

García 把调和数列表扩大到包括小于 10^7 中所有 45 个调和数,他还发现了另外 200 个大的调和数. 除了 1 和完全数外,最小的调和数是 140. 除了 1,有任何调和数是平方数吗? 这样的数有无穷多个吗? 如果是这样,试求小于 x 的这种数的个数的上界和下界. Kanold 证明了它们的密度为 0, Pomerance 则证明了形如 $p^a q^b$(p,q 为素数)的调和数是偶完全数. 如果 $n = p^a q^b r^c$ 是调和数,它是偶的吗?

调和平均取什么样的值? 可能不取 4,12,16,18,20,22,…它取到 23 吗? Ore 猜想每个调和数都是偶数,这将蕴含不存在奇完全数!

Bateman, Erdös, Pomerance 和 Straus 证得使 $\sigma(n)/d(n)$ 取整数值的 n 的集合之密度为 1,使 $\sigma(n)/d(n)^2$ 取整数值的 n 的集合之密度为 $\frac{1}{2}$,不超过 x 的形如 $\sigma(n)/d(n)$ 的有理数 r 的个数为 $o(x)$. 他们希望求出

$$\frac{1}{x}\sum 1$$

的渐近公式,求和取过所有不超过 x 且使 $d(n)$ 不整除 $\sigma(n)$ 的整数 n. 他们还注意到使 $d(n)$ 整除 $s(n)=\sigma(n)-n$ 的整数 n 的密度为 0,因为对几乎所有的 n, $d(n)$ 和 $\sigma(n)$ 都可以被 2 的高次幂整除,而 n 只能被 2 的低次幂整除.

Benkoski 称一个数为奇异数(weird),如果它是过剩数但不是伪完全数. 例如 70 不是

$$1+2+5+7+10+14+35=74$$

的任何子集的和. 在小于一百万的整数中有 24 个本原奇异数: 70, 836, 4030, 5830, 7192, …. 非本原的奇异数有 $70p$(p 为素数且 $p>\sigma(70)=144$), $836p$($p=421,487,491$ 或 p 是 $\geqslant 557$ 的素数)以及 $7192 \cdot 31$. Kravitz 发现了一些大的奇异数, Benkoski 和 Erdös 证明了其密度为正. 这里有一些未解决的问题: 是否存在无穷多个

本原过剩数,它们也是奇异数? 每个奇过剩数都是伪完全数吗(即不是奇异数)? 对奇异数 n,$\sigma(n)/n$ 能否任意大? Benkoski 和 Erdös 猜想最后那个问题的答案是否定的,Erdös 还对最后两个问题的解答分别悬赏 10 美元和 25 美元.

他还问是否有适合下述条件的所谓外奇异数(extra-weird number)n 存在:$\sigma(n)>3n$,n 不能用两种方式(无重复)表成 n 的不同因子之和. 例如,180 不附合条件,虽然有 $\sigma(180)=546$,$180=30+60+90$,而且它还是它的除了 6 以外的所有其他因子之和.

一个数被称为多重完全数(multiply perfect),或重完全数(multiperfect),或 k-重完全数(k-fold perfect),如果 $\sigma(n)=kn$(k 为整数). 例如,通常的完全数是 2-重完全数,120 是一个 3-重完全数. Dickson 的 *History of the Theory of Numbers* 记录了长时期以来人们对这种数的兴趣. Lehmer 指出:如果 n 为奇数,那么仅当 $2n$ 是 3-重完全数时 n 才是完全数.

Selfridge 和其他人注意到恰有 6 个已知的 3-重完全数,它们形如 2^h-1($h=4,6,9,10,14,15$). 例如,其中第三个数可写成

$$\sigma(2^8\cdot7\cdot73\cdot37\cdot19\cdot5)=(2^9-1)(2^3)(37\cdot2)(19\cdot2)(5\cdot2^2)(2\cdot3).$$

对 36 个已知的 4-重完全数来说似乎也有类似的说明,其中最后那个数是由 Poulet 早在 1929 年就已经发表了.

多年来 k 的最大已知的值是 8,对此 Alan L. Brown 给出了 3 个例子,Franqui 和 García 给出另外两个. Stephen Gretton 找到了大批 3-重完全数,还有许多 5-重,6-重,7-重完全数,还有一个 8-重完全数,即

$$2^{62}\cdot3^{15}\cdot5^9\cdot7^7\cdot11^3\cdot13^3\cdot17^2\cdot19\cdot23\cdot29\cdot31^2\cdot37\cdot41\cdot43\cdot53\cdot61^2\cdot71^2\cdot73\cdot83\cdot89\cdot97^2\cdot127\cdot193\cdot283\cdot307\cdot317\cdot331\cdot337\cdot487\cdot521^2\cdot601\cdot1201\cdot1279\cdot2557\cdot3169\cdot5113\cdot92737\cdot649567$$

相信它是这种数中最小的一个.

1992 年末和 1993 年初 Fred Helenius 对 $k=9$ 发现了好几个例子,最小的是

$2^{114}\cdot3^{35}\cdot5^{17}\cdot7^{12}\cdot11^{4}\cdot13^{5}\cdot17^{3}\cdot19^{8}\cdot23^{2}\cdot29^{2}\cdot31^{2}\cdot37^{4}\cdot41\cdot43\cdot47^{2}\cdot53\cdot61^{2}\cdot67\cdot71\cdot73\cdot79^{2}\cdot83^{2}\cdot89^{2}\cdot97\cdot103\cdot109\cdot127\cdot131^{2}\cdot151\cdot157\cdot167\cdot179^{2}\cdot197\cdot211\cdot227\cdot331\cdot347\cdot367\cdot379\cdot443\cdot523\cdot599\cdot709\cdot757\cdot829\cdot1151\cdot1699\cdot1789\cdot2003\cdot2179\cdot2999\cdot3221\cdot4271\cdot4357\cdot4603\cdot5167\cdot8011\cdot8647\cdot8713\cdot14951\cdot17293\cdot21467\cdot29989\cdot110563\cdot178481\cdot530713\cdot672827\cdot4036961\cdot218834597\cdot16148168401\cdot151871210317\cdot2646507710984041.$

问题是 k 可以大到我们希望的那样吗? Erdös 猜想 $k=o(\ln\ln n)$. 甚至有人认为,对 $k\geqslant3$ 仅有有限多个 k-重完全数.

Rich Schroeppel 编写了一个尽可能完全的多重完全数表,对于那些相信自己发现了新的多重完全数的人,可以用他的表来作检查.写好本节头三段时,Shigeru Nakamura 把我的注意力吸引到 Motoji Yoshitake 的工作,他列出了 3 个 5-重完全数,30 个 6-重完全数,35 个 7-重完全数和 8 个 8-重完全数.其中的 2+20+8+0 个归功于 Carmichael, Mason 或 Cunningham. 他的 8-重完全数中有一个是由 Brown 给出的,另外有一个是在此数中用 $19^4\cdot151\cdot911$ 替换 $19^2\cdot127$ 得到的.这一代换是由 Cunningham 在 1902 年发现的,它可以应用到 Carmichael-Mason 的表中,从而给出 50 个重完全数.他还注意到,Carmichael 和 Mason 误把 $137561=151\cdot911$ 和 $485581=277\cdot1753$ 当成了素数. 1992 年我们已经知道 700 个 k-重完全数($k\geqslant3$). 1993 年 1 月,这个数字扩大到 1150 个,从 Fred Helenius 的发现中我们看到有 114 个 7-重完全数,327 个 8-重完全数和 2 个 9-重完全数.他每个月不断发现一些新的数,因此,要想让本书的这一节赶上时代比让本书其余部分赶上时代就更不可能了.到三月份,这种数的总数已接近 1300 个,1993 年 9 月 8 日 Schroepel 的一封信的附言中给出 1526 个,而到他次日寄出这封信时该数已达 1605 个.

若 n 是一个奇的 3-重完全数,则 McDaniel, Cohen, Kishore, Bugulov, Kishore, Cohen 和 Hagis, Reidlinger 以及 Kishore 分别证明了 $\omega(n)\geqslant9,9,10,11,11,11,12$ 和 12. Beck 和 Najar,

Alexander,以及 CohenHagis 证明了 $n>10^{50},10^{60}10^{70}$. Cohen 和 Hagis 证明了 n 的最大素因子至少是 100129,第二大素因子至少是 1009.

Shigeru Nakamura 写道:1966 年 Bugulov 证明了奇 k-重完全数至少有 ω 个不同的素因子,其中 $(k,\omega)=(3,11),(4,21),(5,54)$(*MR* 37 #5139 及 rNT A32-96 中的叙述并不正确). Nakamura 宣称他证明了:对偶的 k-重完全数有

$$\omega>\max\{k^3/81+\frac{5}{3},k^5/2500+2.9,k^{10}/(14\cdot 10^8)+2.9999\},$$

而对奇的 k-重完全数有

$$\omega>\max\{k^5/60+\frac{47}{12},k^5/50-20.8,737k^{10}/10^9+11.5\}.$$

这些改进了 Cohen 和 Hendy 以及 Reidlinger 的结果;对 Bugulov 的结果,他也给出了改进:$(k,\omega)=(4,23),(5,56),(6,142),(7,373)$.

Minoli 和 Bear 称 n 是 k-超完全数(k-hyperperfect),如果 $n=1+k\sum d_i$,这里求和经过所有真因子,$1<d_i<n$,从而有 $k\sigma(n)=(k+1)n+k-1$. 例如,21,2133 和 19521 是 2-超完全数,325 是 3-超完全数.他们猜想对每个 k 有 k-超完全数存在.

Ron Graham 问是否由 $s(n)=\lfloor n/2\rfloor$ 可推出 n 或为 2,或为 3 的幂?

Erdös 令 $f(n)$ 表示使得对某个 k 有 $n=\sum_{i=1}^{k}d_i$ 成立的最小整数,这里 $1=d_1<d_2<\cdots<d_l=f(n)$ 是 $f(n)$ 的因子的增加序列. 是否有 $f(n)=o(n)$? 或者它只对几乎所有的 n 为真,且 $\limsup f(n)/n=\infty$?

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f(n)$	1	—	2	3	—	5	4	7	15	12	21	6	9	13

n	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$f(n)$	8	12	30	10	42	19	18	20	57	14	36	46	30	12

Erdös 定义 n_k 为具有下述性质的最小整数:如果把 n_k 的真因子分成 k 个类,n_k 总是等于同一个类中不同因子的和. 显然 $n_1=6$,但是他甚至不能证明 n_2 的存在.

参考文献

H. Abbott, C. E. Aull, Ezra Brown & D. Suryanarayana, Quasiperfect numbers, *Acta Arith.*, **22**(1973) 439–447; *MR* **47** #4915; corrections, **29**(1976) 427–428.

Leon Alaoglu & Paul Erdős, On highly composite and similar numbers, *Trans. Amer. Math. Soc.*, **56**(1944) 448–469; *MR* **6**, 117b.

L. B. Alexander, Odd triperfect numbers are bounded below by 10^{60}, M.A. thesis, East Carolina University, 1984.

M. M. Artuhov, On the problem of odd h-fold perfect numbers, *Acta Arith.*, **23**(1973) 249–255.

Paul T. Bateman, Paul Erdős, Carl Pomerance & E.G. Straus, The arithmetic mean of the divisors of an integer, in *Analytic Number Theory* (*Philadelphia, 1980*) 197–220, *Lecture Notes in Math.*, **899**, Springer, Berlin - New York, 1981; *MR* **84**b:10066.

Walter E. Beck & Rudolph M. Najar, A lower bound for odd triperfects, *Math. Comput.*, **38**(1982) 249–251.

S. J. Benkoski, Problem E2308, *Amer. Math. Monthly*, **79**(1972) 774.

S. J. Benkoski & P. Erdős, On weird and pseudoperfect numbers, *Math. Comput.*, **28**(1974) 617–623; *MR* **50** #228; corrigendum, S. Kravitz, **29**(1975) 673.

Alan L. Brown, Multiperfect numbers, *Scripta Math.*, **20**(1954) 103–106; *MR* **16**, 12.

E. A. Bugulov, On the question of the existence of odd multiperfect numbers (Russian), *Kabardino-Balkarsk. Gos. Univ. Ucen. Zap.*, **30**(1966) 9–19.

David Callan, Solution to Problem 6616, *Amer. Math. Monthly*, **99**(1992) 783–789.

R. D. Carmichael & T. E. Mason, Note on multiply perfect numbers, including a table of 204 new ones and the 47 others previously published, *Proc. Indiana Acad. Sci.*, **1911** 257–270.

Paolo Cattaneo, Sui numeri quasiperfetti, *Boll. Un. Mat. Ital.*(3), **6**(1951) 59–62; *Zbl.* **42**, 268.

Graeme L. Cohen, On odd perfect numbers II, multiperfect numbers and quasiperfect numbers, *J. Austral. Math. Soc. Ser. A*, **29**(1980) 369–384; *MR* **81m**:10009.

Graeme L. Cohen, The non-existence of quasiperfect numbers of certain forms, *Fibonacci Quart.*, **20**(1982) 81–84.

Graeme L. Cohen, On primitive abundant numbers, *J. Austral. Math. Soc. Ser. A*, **34**(1983) 123–137.

Graeme L. Cohen, Primitive α-abundant numbers, *Math. Comput.*, **43**(1984) 263–270.

Graeme L. Cohen, Stephen Gretton and his multiperfect numbers, Internal Report No. 28, School of Math. Sciences, Univ. of Technology, Sydney, Australia, Oct 1991.

G. L. Cohen & P. Hagis, Results concerning odd multiperfect numbers, *Bull. Malaysian Math. Soc.*, **8**(1985) 23–26.

G. L. Cohen & M. D. Hendy, On odd multiperfect numbers, *Math. Chronicle*, **9**(1980) 120–136; **10**(1981) 57–61.

Philip L. Crews, Donald B. Johnson & Charles R. Wall, Density bounds for the sum of divisors function, *Math. Comput.*, **26**(1972) 773–777; *MR* **48** #6042; Errata **31**(1977) 616; *MR* **55** #286.

J. T. Cross, A note on almost perfect numbers, *Math. Mag.*, **47**(1974) 230–231.

P. Erdős, On the density of the abundant numbers, *J. London Math. Soc.*, **9**(1934) 278–282.

P. Erdős, Problems in number theory and combinatorics, *Congressus Numerantium XVIII, Proc. 6th Conf. Numerical Math. Manitoba*, 1976, 35–58 (esp. pp. 53–54); *MR* **80e**:10005.

Benito Franqui & Mariano García, Some new multiply perfect numbers, *Amer. Math. Monthly*, **60**(1953) 459–462; *MR* **15**, 101.

Benito Franqui & Mariano García, 57 new multiply perfect numbers, *Scripta Math.*, **20**(1954) 169–171 (1955); *MR* **16**, 447.

Mariano García, A generalization of multiply perfect numbers, *Scripta Math.*, **19**(1953) 209–210; *MR* **15**, 199.

Mariano García, On numbers with integral harmonic mean, *Amer. Math. Monthly*, **61** (1954) 89–96; *MR* **15**, 506, 1140.

Peter Hagis, The third largest prime factor of an odd multiperfect number exceeds 100, *Bull. Malaysian Math. Soc.*, **9**(1986) 43–49.

Peter Hagis, A new proof that every odd triperfect number has at least twelve prime factors, *A tribute to Emil Grosswald: number theory and related analysis*, 445-450 *Contemp. Math.*, **143** Amer. Math. Soc., 1993. 43–49.

Peter Hagis & Graeme L. Cohen, Some results concerning quasiperfect numbers, *J. Austral. Math. Soc. Ser. A*, **33**(1982) 275–286.

B. E. Hardy & M. V. Subbarao, On hyperperfect numbers, Proc. 13th Manitoba Conf. Numer. Math. Comput., *Congressus Numerantium*, **42**(1984) 183–198; *MR* **86c**:11006.

B. Hornfeck & E. Wirsing, Über die Häufigkeit vollkommener Zahlen, *Math. Ann.*, **133**(1957) 431–438; *MR* **19**, 837; see also **137**(1959) 316–318; *MR* **21** #3389.

R. P. Jerrard & Nicholas Temperley, Almost perfect numbers, *Math. Mag.*, **46** (1973) 84–87.

H.-J. Kanold, Über mehrfach vollkommene Zahlen, *J. reine angew. Math.*, **194** (1955) 218–220; II **197**(1957) 82–96; *MR* **17**, 238; **18**, 873.

H.-J. Kanold, Über das harmonische Mittel der Teiler einer natürlichen Zahl, *Math. Ann.*, **133**(1957) 371–374.

H.-J. Kanold, Einige Bemerkungen über vollkommene und mehrfach vollkommene Zahlen, *Abh. Braunschweig. Wiss. Ges.*, **42**(1990/91) 49–55; *MR* **93c**: 11002.

David G. Kendall, The scale of perfection, *J. Appl. Probability*, **19A**(1982) 125–138; *MR* **83d**:10007.

Masao Kishore, Odd triperfect numbers, *Math. Comput.*, **42**(1984) 231–233; *MR* **85d**:11009.

Masao Kishore, Odd triperfect numbers are divisible by eleven distinct prime factors, *Math. Comput.*, **44** (1985) 261–263; *MR* **86k**:11007.

Masao Kishore, Odd triperfect numbers are divisible by twelve distinct prime factors, *J. Autral. Math. Soc. Ser. A*, **42**(1987) 173–182.

Masao Kishore, Odd integers N with 5 distinct prime factors for which $2 - 10^{-12} < \sigma(N)/N < 2 + 10^{-12}$, *Math. Comput.*, **32**(1978) 303–309.

M. S. Klamkin, Problem E1445*, *Amer. Math. Monthly*, **67**(1960) 1028; see also **82**(1975) 73.

Sidney Kravitz, A search for large weird numbers, *J. Recreational Math.*, **9**(1976-77) 82–85.

Richard Laatsch, Measuring the abundancy of integers, *Math. Mag.*, **59** (1986) 84–92.

A. Mąkowski, Remarques sur les fonctions $\theta(n)$, $\phi(n)$ et $\sigma(n)$, *Mathesis*, **69**(1960) 302–303.

A. Mąkowski, Some equations involving the sum of divisors, *Elem. Math.*, **34**(1979) 82; *MR* **81b**:10004.

Wayne L. McDaniel, On odd multiply perfect numbers, *Boll. Un. Mat. Ital.* (4), **3**(1970) 185–190; *MR* **41** #6764.

W. H. Mills, On a conjecture of Ore, *Proc. Number Theory Conf.*, Boulder CO, 1972, 142–146.

D. Minoli, Issues in non-linear hyperperfect numbers, *Math. Comput.*, **34** (1980) 639–645; *MR* **82c**:10005.

Daniel Minoli & Robert Bear, Hyperperfect numbers, *Pi Mu Epsilon J.*, **6**#3(1974-75) 153–157.

Shigeru Nakamura, On k-perfect numbers (Japanese), *J. Tokyo Univ. Merc. Marine(Nat. Sci.)*, **33**(1982) 43–50.

Shigeru Nakamura, On some properties of $\sigma(n)$, *J. Tokyo Univ. Merc. Marine(Nat. Sci.)*, **35**(1984) 85–93.

Shigeru Nakamura, On multiperfect numbers, (unpublished typescript).

Oystein Ore, On the averages of the divisors of a number, *Amer. Math. Monthly*, **55**(1948) 615–619.

Seppo Pajunen, On primitive weird numbers, *A collection of manuscripts related to the Fibonacci sequence*, 18th anniv. vol., Fibonacci Assoc., 162–166.

Carl Pomerance, On a problem of Ore: Harmonic numbers (unpublished typescript); see Abstract *709-A5, *Notices Amer. Math. Soc.*, **20**(1973) A-648.

Carl Pomerance, On multiply perfect numbers with a special property, *Pacific J. Math.*, **57**(1975) 511–517.

Carl Pomerance, On the congruences $\sigma(n) \equiv a \bmod n$ and $n \equiv a \bmod \phi(n)$, *Acta Arith.*, **26**(1975) 265–272.

Paul Poulet, *La Chasse aux Nombres*, Fascicule I, Bruxelles, 1929, 9–27.

Problem B-6, William Lowell Putnam Mathematical Competition, 1976-12-04.

Problem 14, *Abacus*, **1**(1984) 93.

Herwig Reidlinger, Über ungerade mehrfach vollkommene Zahlen [On odd multiperfect numbers], *Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II*, **192**(1983) 237–266; *MR* **86d**:11018.

Herman J. J. te Riele, Hyperperfect numbers with three different prime factors, *Math. Comput.*, **36**(1981) 297–298.

Neville Robbins, A class of solutions of the equation $\sigma(n) = 2n + t$, *Fibonacci Quart.*, **18**(1980) 137–147 (misprints in solutions for $t = 31, 84, 86$).

M. Satyanarayana, Bounds of $\sigma(N)$, *Math. Student*, **28**(1960) 79–81.

H. N. Shapiro, Note on a theorem of Dickson, *Bull. Amer. Math. Soc.*, **55**(1949) 450–452.

H. N. Shapiro, On primitive abundant numbers, *Comm. Pure Appl. Math.*, **21** (1968) 111–118.

W. Sierpiński, Sur les nombres pseudoparfaits, *Mat. Vesnik*, **2**(17)(1965) 212–213; *MR* **33** #7296.

W. Sierpiński, *Elementary Theory of Numbers* (ed. A. Schinzel), PWN–Polish Scientific Publishers, Warszawa, 1987, pp. 184–186.

D. Suryanarayana, Quasi-perfect numbers II, *Bull. Calcutta Math. Soc.*, **69** (1977) 421–426; *MR* **80m**:10003.

Charles R. Wall, The density of abundant numbers, Abstract 73T–A184, *Notices Amer. Math. Soc.*, **20**(1973) A-472.

Charles R. Wall, A Fibonacci-like sequence of abundant numbers, *Fibonacci Quart.*, **22**(1984) 349; *MR* **86d**:11018.

Charles R. Wall, Phillip L. Crews & Donald B. Johnson, Density bounds for the sum of divisors function, *Math. Comput.*, **26**(1972) 773–777.

Motoji Yoshitake, Abundant numbers, sum of whose divisors is equal to an integer times the number itself (Japanese), *Sūgaku Seminar*, **18**(1979) no. 3, 50–55.

Andreas & Eleni Zachariou, Perfect, semi-perfect and Ore numbers, *Bull. Soc. Math. Grèce*(N.S.), **13**(1972) 12–22; *MR* **50** #12905.

B3. 单完全数

如果 d 整除 n，$d \perp n/d$，则称 d 是 n 的一个单因子(unitary divisor). 如果数 n 是它的除去自身以外的单因子之和，则称之为单完全数(unitary perfect number). 没有奇的单完全数存在. 而 Subbarao 猜想只有有限多个偶的单完全数存在. Subbarao, Carlitz 和 Erdös 每人为解决此问题都悬赏 10 美元，Subbarao 对每个新的例子还悬赏 10 美分. 若 $n = 2^a m$(其中 m 为奇数，且有 r 个不同的素因子)，则 Subbarao 和其他人证明了：除了 $2\cdot3, 2^2\cdot3\cdot5, 2\cdot3^2\cdot5$ 以及 $2^6\cdot3\cdot5\cdot7\cdot13$ 外，没有单完全数满足 $a \leqslant 10$ 或者 $r \leqslant 6$. S. W. Graham 证明了：上述第一和第三个数是仅有的形如 $2^a m$(m 为无平方因子的奇数)的单完全数；而 Jennifer DeBoer 则证明了：

上面的第二个数是仅有的形如 2^a3^2m（$m\perp 6$ 且无平方因子）的单完全数.

Wall 找到了单完全数

$$2^{18}\cdot 3\cdot 5^4\cdot 7\cdot 11\cdot 13\cdot 19\cdot 37\cdot 79\cdot 109\cdot 157\cdot 313,$$

他证明了这是第五个这样的数. 他还可以证明任何其他的单完全数都有一个大于 2^{15}的因子. Frey 证明了：若 $N=2^m\cdot p_1^{a_1}\cdots p_r^{a_r}$ 是单完全数，且满足 $N\perp 3$，则必有 $m>144$，$r>144$ 以及 $N>10^{440}$.

Peter Hagis 研究了单的重完全数(unitary multiperfect number)：这种数没有奇的. 用 $\sigma^*(n)$表示 n 的单因子之和. 如果 $\sigma^*(n)=kn$ 且 n 有 t 个不同的奇素因子，那么由 $k=4$ 或 6 即可推出有 $n>10^{110}$，$t\geqslant 51$ 以及 $2^{49}\mid n$；而由 $k\geqslant 8$ 即可推出有 $n>10^{663}$以及 $k\geqslant 247$；又由 $k\geqslant 5$ 为奇数即可推出有 $n>10^{461}$，$t\geqslant 166$ 以及 $2^{166}\mid n$.

Cohen 称整数 n 的一个因子 d 为 n 的一个 1-元因子(1-ary divisor)，如果 $d\perp n/d$；称 d 为 n 的一个 k-元因子(k-ary divisor)($k>1$)并记为 $d\mid_k n$，如果 d 和 n/d 的最大($k-1$)-元公因子为 1（记为$(d,n/d)_{k-1}=1$）. 根据这一记号，$d\mid n$ 和 $d\parallel n$ 可以写成 $d\mid_0 n$ 和 $d\mid_1 n$. 他还称 p^x 是 p^y($y>0$)一个**无穷元因子**(infinitary divisor)，如果有 $p^x\mid_{y-1}p^y$. 这就对早先的概念提出了无穷元类似概念. 用 $\sigma_\infty(n)$表示 n 的无穷元因子之和. 他发现了 14 个无穷元完全数，即满足 $\sigma_\infty(n)=kn$ 及 $k=2$ 的数；对 $k=3$ 发现了 13 个这样的数；对 $k=4$ 发现了 7 个这样的数；而对 $k=5$ 则发现了 2 个这样的数. 没有这样的奇数. 他猜想：没有不被 3 整除的无穷元重完全数.

注意，Suryanarayana(他也用了"k-元因子"这一术语)和 Alladi 给出了单因子的不同的推广

参考文献

K. Alladi, On arithmetic functions and divisors of higher order, *J. Austral. Math. Soc. Ser. A*, **23**(1977) 9–27.

Graeme L. Cohen, On an integer's infinitary divisors, *Math. Comput.*, **54** (1990) 395–411.

Graeme Cohen & Peter Hagis, Arithmetic functions associated with the infinitary divisors of an integer, *Internat. J. Math. Math. Sci.*, (to appear).

J. L. DeBoer, On the non-existence of unitary perfect numbers of certain type, *Pi Mu Epsilon J.* (submitted).

H. A. M. Frey, Über unitär perfekte Zahlen, *Elem. Math.*, **33**(1978) 95–96; *MR* **81a**:10007.

S. W. Graham, Unitary perfect numbers with squarefree odd part, *Fibonacci Quart.*, **27**(1989) 317–322; *MR* **90i**:11003.

Peter Hagis, Lower bounds for unitary multiperfect numbers, *Fibonacci Quart.*, **22**(1984) 140–143; *MR* **85j**:11010.

Peter Hagis, Odd nonunitary perfect numbers, *Fibonacci Quart.*, **28** (1990) 11–15; *MR* **90k**:11006.

Peter Hagis & Graeme Cohen, Infinitary harmonic numbers, *Bull. Austral. Math. Soc.*, **41**(1990) 151–158; *MR* **91d**:11001.

József Sándor, On Euler's arithmetical function, *Proc. Alg. Conf. Braşov 1988*, 121–125.

V. Siva Rama Prasad & D. Ram Reddy, On unitary abundant numbers, *Math. Student*, **52**(1984) 141–144 (1990) *MR* **91m**:11002.

V. Siva Rama Prasad & D. Ram Reddy, On primitive unitary abundant numbers, *Indian J. Pure Appl. Math.*, **21**(1990) 40–44; *MR* **91f**:11004.

M. V. Subbarao, Are there an infinity of unitary perfect numbers? *Amer. Math. Monthly*, **77**(1970) 389–390.

M. V. Subbarao & D. Suryanarayana, Sums of the divisor and unitary divisor functions, *J. reine angew. Math.*, **302**(1978) 1–15; *MR* **80d**:10069.

M. V. Subbarao & L. J. Warren, Unitary perfect numbers, *Canad. Math. Bull.*, **9**(1966) 147–153; *MR* **33** #3994.

M. V. Subbarao, T. J. Cook, R. S. Newberry & J. M. Weber, On unitary perfect numbers, *Delta*, **3**#1(Spring 1972) 22–26.

D. Suryanarayana, The number of k-ary divisors of an integer, *Monatsh. Math.*, **72**(1968) 445–450.

Charles R. Wall, The fifth unitary perfect number, *Canad. Math. Bull.*, **18**(1975) 115–122. See also *Notices Amer. Math. Soc.*, **16**(1969) 825.

Charles R. Wall, Unitary harmonic numbers, *Fibonacci Quart.*, **21**(1983) 18–25.

Charles R. Wall, On the largest odd component of a unitary perfect number, *Fibonacci Quart.*, **25**(1987) 312–316; *MR* **88m**:11005.

B4. 亲 和 数

两个不相等的数 m 和 n 称为**亲和的**(amicable),如果每个数都是另一个数的所有真因子之和,即 $\sigma(m)=\sigma(n)=m+n$.已知有几千个这样的数对.最小的一对亲和数中较小的那个数是 220(它出现在《创世纪》第 32 章 14 行中),自那时以来,亲和数使希腊人、阿拉伯人及其他许多国家的人着了迷.有关亲和数的历史可以看 Lee 和 Madachy 的文章.根据英国国王 James 一世的钦译《圣经》,世纪初创是把 200 个雌性动物和 20 个雄性动物融合在一起而成功的.Aviezri Fraenkel 在《圣经》的首五卷中写下了这些内容,它们出现在第 32 章 15 行中(此处原书有误,但根据作者意见,未作改动);在《以斯拉书》第 8 章 20 行以及《历王记》第 15 章 6 行中更加令人信服地给出了数 220;在《尼希米记》第 11 章 18 行中给出了 284(它是最小的那对亲和数中较大的那个数——译者注).他注意到这三处是密切相关的:他们全都与 Levi(Levi 是《创世纪》中的人物,他是 Jacob 与 Leah 的第三个儿子——译者注)的部落有关,这个部落的名字源于 Levi 的母亲要与他的父亲亲和的愿望(《创世纪》第 29 章 34 行).

不知道是否有无穷多个亲和数,但人们相信如此.实际上 Erdös 猜想:满足 $m<n<x$ 的这种数对的个数 $A(x)$ 至少有 $x^{1-\epsilon}$ 个.他改进了 Kanold 的一个结果,由此证明了 $A(x)=o(x)$.他的方法可以用来证明 $A(x)\leqslant cx/\ln\ln\ln x$.Pomerance 得到了进一步的改进

$$A(x)\leqslant x\exp\{-c(\ln\ln\ln x\ln\ln\ln\ln x)^{1/2}\}.$$

Erdös 猜想对每个 k 有 $A(x)=o(x/(\ln x)^k)$,而 Pomerance 则证明了更强的结果

$$A(x)\leqslant x\exp\{-(\ln x)^{1/3}\}.$$

这蕴含亲和数的倒数之和有限,这是一个新近才知道的事实.他还注意到,他的证明可以经过修改用来证明更强一点的结果

$$A(x) \ll x\exp\{-c(\ln\ln\ln x)^{1/3}\}.$$

Herman te Riele 找出了较小的那个亲和数小于 10^{10} 的所有 1427 对亲和数. 他注意到量 $A(x)(\ln x)^3/x^{1/2}$ 与 147.6 相当接近,但是我怀疑更强有力的方法会要求指数 1/2 增加到非常接近 1. D. Moews 和 P. C. Moews 继续这一搜寻亲和数的工作直到超过 $2\cdot10^{11}$. 通过 Battiato 和其他人的努力,已经找到 40 万对亲和数.

te Riele 发现了一些很大的亲和数对,它们有 32、40、81 和 152 位数字;Kaplansky 在 1975 年的 *Encyclopedia Britannica Yearbook* 的"数学"条目中提到了他发现的这些数. 而以前已知最大的亲和数对只有 25 位数字. 最近,te Riele 通过一张有 92 个已知亲和数对的"母表"构造出 2000 多对有多到 38 位数字的新亲和数对,以及 5 对有 239 位到 282 位数字的新亲和数对. 1993 年中期已知最大的亲和数对有 1041 位数字:

$$(2^9p^{20}q_1rstu, 2^9p^{20}q_2v)$$

其中 $p=5661346302015448219060051$;$q_1$ 和 q_2 形如 $bc^{20}-1$,这里,$b_1=5797874220719830725124352$, $b_2=5531348900141215019827200$, $c=5661346302015448219060051$;又 $r=569$, $s=5039$, $t=1479911$, $u=30636732851$;且 $v=1365279187043825060643301$. 这是由 Holger Wiethaus 发现的,他是我 1988 年在 Dortmund 的学生.

Elvin J. Lee 给出过好几个判别形如 $(2^npq, 2^nrs)$ 的亲和数的方法,其中 p, q, r 是适当形状的素数. 例如

$p=3\cdot2^{n-1}-1, q=35\cdot2^{n+1}-29, r=7\cdot2^{n-1}-1, s=15\cdot2^{n+1}-13$,

但是同时找到 4 个这样的素数是很难得的.

Borho, Hoffman 和 te Riele 取得了很大的进展,他们都用到了推广的 Thabit 法则加上实际计算. 上面提到的 1427 对亲和数中,除了 17 对满足 $m+n\equiv0\bmod9$ 的以外,其余全部都是由他们发现的. 最小的例外是 Poulet 的数对

$$2^4\cdot331\cdot\begin{cases}19\cdot6619\\199\cdot661\end{cases}$$

它们满足 $m+n\equiv 5 \bmod 9$, te Riele 则给出了头一批满足 m,n 为偶数且 $m+n\equiv 3 \bmod 9$ 的例子：

$$2^4\cdot\begin{cases}19^2\cdot 103\cdot 1627\\ 3847\cdot 16763\end{cases}\quad 和\quad 2^2\cdot 19\cdot\begin{cases}13^2\cdot 37\cdot 43\cdot 139\\ 41\cdot 151\cdot 6709\end{cases}$$

还不知道是否有使 m,n 奇偶性相反或使 $m\perp n$ 的亲和数对存在. Bratley 和 Mckay 猜想:所有奇亲和数对的两个数都可被 3 整除,但 Battiato 和 Borho 造出了位数从 36 到 73 的 15 个反例. 在一封写于 1987 年 5 月 15 日的信中, te Riele 宣布得到一个 33 位的例子：

$$5\cdot 7^2\cdot 11^2\cdot 13\cdot 17\cdot 19^3\cdot 23\cdot 37\cdot 181$$
$$\cdot\begin{cases}101\cdot 8643\cdot 1947938229\\ 365147\cdot 47303071129.\end{cases}$$

这是否是满足此种条件的最小的数对? 是否存在奇亲和数对,它恰只有一个数能被 3 整除?

Charles Wall 的一个早先的猜想是奇亲和数对必模 4 不同余. 他说,这一猜想为真即蕴含不存在奇完全数. 故寻找一个反例可能比试图证明它要更为恰当.

在 1978 年的最佳图书 *Mathematical Magic Show* p. 169 上 Martin Gardner 对亲和数的数字根(所谓数字根,系指关于模 9 的剩余类——译者注)做出一个猜想. Lee 证明了: 如果 $(2^n pqr, 2^n stu)$ 是一对亲和数,其和不被 9 整除,则每一个数都同余于 $7 \bmod 9$. 由此他部分地证实了上述猜想.

Peter Hagis 和 Mariano García 研究了单亲和数(unitary amicable number),他们给出了 82 对这样的数.

参考文献

J. Alanen, O. Ore & J. G. Stemple, Systematic computations on amicable numbers, *Math. Comput.*, **21**(1967) 242–245; *MR* **36** #5058.

M. M. Artuhov, On some problems in the theory of amicable numbers (Russian), *Acta Arith.*, **27**(1975) 281–291.

S. Battiato, *Über die Produktion von 37803 neuen befreundeten Zahlenpaaren mit der Brütermethode*, Master's thesis, Wuppertal, June 1988.

S. Battiato & W. Borho, Are there odd amicable numbers not divisible by three? *Math. Comput.*, **50**(1988) 633–636; *MR* **89c**:11015.

W. Borho, On Thabit ibn Kurrah's formula for amicable numbers, *Math. Comput.*, **26**(1972) 571–578.

W. Borho, Befreundete Zahlen mit gegebener Primteileranzahl, *Math. Ann.*, **209**(1974) 183–193.

W. Borho, Eine Schranke für befreundete Zahlen mit gegebener Teileranzahl, *Math. Nachr.*, **63**(1974) 297–301.

W. Borho, Some large primes and amicable numbers, *Math. Comput.*, **36** (1981) 303–304.

W. Borho & H. Hoffmann, Breeding amicable numbers in abundance, *Math. Comput.*, **46**(1986) 281–293.

P. Bratley & J. McKay, More amicable numbers, *Math. Comput.*, **22**(1968) 677–678; *MR* **37** #1299.

P. Bratley, F. Lunnon & J. McKay, Amicable numbers and their distribution, *Math. Comput.*, **24**(1970) 431–432.

B. H. Brown, A new pair of amicable numbers, *Amer. Math. Monthly*, **46** (1939) 345.

Patrick Costello, Four new amicable pairs, *Notices Amer. Math. Soc.*, **21** (1974) A-483.

Patrick Costello, Amicable pairs of Euler's first form, *Notices Amer. Math. Soc.*, **22**(1975) A-440.

Patrick Costello, Amicable pairs of the form $(i, 1)$, *Math. Comput.*, **56**(1991) 859–865; *MR* **91k**:11009.

P. Erdős, On amicable numbers, *Publ. Math. Debrecen*, **4**(1955) 108–111; *MR* **16**, 998.

P. Erdős & G. J. Rieger, Ein Nachtrag über befreundete Zahlen, *J. reine angew. Math.*, **273**(1975) 220.

E. B. Escott, Amicable numbers, *Scripta Math.*, **12**(1946) 61–72; *MR* **8**, 135.

M. García, New amicable pairs, *Scripta Math.*, **23**(1957) 167–171; *MR* **20** #5158.

Mariano García, New unitary amicable couples, *J. Recreational Math.*, **17** (1984-5) 32–35.

Mariano García, K-fold isotopic amicable numbers, *J. Recreational Math.*, **19** (1987) 12–14

Mariano García, Some useful substitutions for finding amicable numbers (preprint March 1987).

Mariano García, Favorable conditions for amicability, *Hostos Community Coll. Math. J.*, New York, Spring 1989, 20–25.

A. A. Gioia & A. M. Vaidya, Amicable numbers with opposite parity, *Amer. Math. Monthly*, **74**(1967) 969–973; correction **75**(1968) 386; *MR* **36** #3711, **37** #1306.

Peter Hagis, On relatively prime odd amicable numbers, *Math. Comput.*, **23**(1969) 539–543; *MR* **40** #85.

Peter Hagis, Lower bounds for relatively prime amicable numbers of opposite parity, *Math. Comput.*, **24**(1970) 963–968.

Peter Hagis, Relatively prime amicable numbers of opposite parity, *Math. Mag.*,

43(1970) 14–20.
Peter Hagis, Unitary amicable numbers, *Math. Comput.*, **25**(1971) 915-918.
H.-J. Kanold, Über die Dichten der Mengen der vollkommenen und der befreundeten Zahlen, *Math. Z.*, **61**(1954) 180–185; *MR* **16**, 337.
H.-J. Kanold, Über befreundete Zahlen I, *Math. Nachr.*, **9**(1953) 243–248; II *ibid.*, **10** (1953) 99–111; *MR* **15**, 506.
H.-J. Kanold, Über befreundete Zahlen III, *J. reine angew. Math.*, **234**(1969) 207–215; *MR* **39** #122.
E. J. Lee, Amicable numbers and the bilinear diophantine equation, *Math. Comput.*, **22**(1968) 181–187; *MR* **37** #142.
E. J. Lee, On divisibility by nine of the sums of even amicable pairs, *Math. Comput.*, **23**(1969) 545–548; *MR* **40** #1328.
E. J. Lee & J. S. Madachy, The history and discovery of amicable numbers, part 1, *J. Recreational Math.*, **5**(1972) 77–93; part 2, 153–173; part 3, 231–249.
O. Ore, *Number Theory and its History*, McGraw-Hill, New York, 1948, p. 89.
Carl Pomerance, On the distribution of amicable numbers, *J. reine angew. Math.*, **293/294**(1977) 217–222; II **325**(1981) 183–188; *MR* **56** #5402, **82m**: 10012.
P. Poulet, 43 new couples of amicable numbers, *Scripta Math.*, **14**(1948) 77.
H. J. J. te Riele, Four large amicable pairs, *Math. Comput.*, **28**(1974) 309–312.
H. J. J. te Riele, On generating new amicable pairs from given amicable pairs, *Math. Comput.*, **42**(1984) 219–223.
Herman J. J. te Riele, New very large amicable pairs, in *Number Theory* Noordwijkerhout 1983, *Springer Lecture Notes in Math.*, **1068**(1984) 210–215.
H. J. J. te Riele, Computation of all the amicable pairs below 10^{10}, *Math. Comput.*, **47**(1986) 361–368 & S9–S40.
H. J. J. te Riele, A new method for finding amicable pairs, in *Mathematics of Computation 1943–1993* (Vancouver, 1993), *Proc. Sympos. Appl. Math.* **43**, Amer. Math. Soc., Providence RI, 1994.
H. J. J. te Riele, W. Borho, S. Battiato, H. Hoffmann & E.J. Lee, *Table of Amicable Pairs between* 10^{10} *and* 10^{52}, Centrum voor Wiskunde en Informatica, Note NM-N8603, Stichting Math. Centrum, Amsterdam, 1986.
Dale Woods, Construction of amicable pairs, #789-10-21, *Abstracts Amer. Math. Soc.*, **3**(1982) 223.

B5. 拟亲和数或匹配数

García 称一对数(m,n)，$m<n$ 为拟亲和的(quasi-amicable)，如果有

$$\sigma(m)=\sigma(n)=m+n+1.$$

例如(48,75)，(140,195)，(1575,1648)，(1050,1925)和(2024，2295)均是. Rufus Isaacs 注意到 m 和 n 中每个数都是另一个数的(去掉 1 及其自身的)所有真因子之和，于是更恰当地称它们为匹

配数(betrothed number).

Małkowski 给出了匹配数的例子以及亲和三数组(amicable triple)

$$\sigma(a)=\sigma(b)=\sigma(c)=a+b+c$$

的例子,例如 $2^2\cdot3^2\cdot5\cdot11$, $2^5\cdot3^2\cdot7$, $2^2\cdot3^2\cdot71$. 类似地,在一封 1992 年 7 月 20 日的信中,Yasutoshi Kohmoto 称数集 $\{a,b,c,d\}$ 为**拟亲和的**(quasi-amicable),如果

$$\sigma(a)=\sigma(b)=\sigma(c)=\sigma(d)=a+b+c+d.$$

作为不是 3 的倍数的例子,他给出

$$a=x\cdot173\cdot1933058921\cdot149\cdot103540742849,$$
$$b=x\cdot173\cdot1933058921\cdot15531111427499,$$
$$c=x\cdot336352252427\cdot149\cdot103540742849,$$
$$d=x\cdot336352252427\cdot15531111427499.$$

其中 x 是数

$$5^9\cdot7^2\cdot11^4\cdot17^2\cdot19\cdot29^2\cdot67\cdot71^2\cdot109\cdot131\cdot139\cdot179\cdot307\cdot431\cdot521\cdot653\cdot1019\cdot1279\cdot2557\cdot3221\cdot5113\cdot5171\cdot6949$$

与一个完全数 $2^{p-1}M_p$($M_p=2^p-1$ 为 Mersenne 素数,见 A3)的乘积($p>3$).

Hagis 和 Lord 找到了满足 $m<10^7$ 的所有 46 对匹配数. 它们全都有相反的奇偶性. 目前还不知道有使 m 和 n 有相同奇偶性的匹配数存在. 如果有的话,则必有 $m>10^{10}$. 如果 $m\perp n$,则 mn 至少包含 4 个不同的素因子,又如果 mn 为奇数,那么 mn 至少包含 21 个不同的素因子.

Beck 和 Najar 称这样的一对数为约化的亲和数对,并把满足

$$\sigma(m)=\sigma(n)=m+n-1$$

的数 m 和 n 称为增长的亲和数对. 他们发现了 11 对增长的亲和数,但在 $n<10^5$ 以内没有发现约化的或增长的单亲和数或交际数(见 B8).

参考文献

Walter E. Beck & Rudolph M. Najar, More reduced amicable pairs, *Fibonacci Quart.*, **15**(1977) 331–332; *Zbl.* **389**.10004.

Walter E. Beck & Rudolph M. Najar, Fixed points of certain arithmetic functions, *Fibonacci Quart.*, **15**(1977) 337–342; *Zbl.* **389**.10005.

Peter Hagis & Graham Lord, Quasi-amicable numbers, *Math. Comput.*, **31** (1977) 608–611; *MR* **55** #7902; *Zbl.* **355**.10010.

M. Lal & A. Forbes, A note on Chowla's function, *Math. Comput.*, **25**(1971) 923–925; *MR* **45** #6737; *Zbl.* **245**.10004.

Andrzej Mąkowski, On some equations involving functions $\phi(n)$ and $\sigma(n)$, *Amer. Math. Monthly*, **67**(1960) 668–670; correction **68**(1961) 650; *MR* **24** #A76.

B6. 真因子序列

既然有些数是过剩数,有些数是不足数,人们自然会问:在作函数 $s(n)=\sigma(n)-n$ 的迭代产生出**真因子序列**(aliquot sequence)$\{s^k(n)\}$, $k=0,1,2,\cdots$时,会发生什么? Catalan 和 Dickson 猜想:所有这样的序列都是有界的,但是现在我们通过合理的讨论,有证据表明:某些序列,可能是那些 n 取偶数的序列是趋向无穷的.对该序列的有界性曾存有怀疑的最小的 n 是 138,然而 D.H. Lehmer 最终证明了:在达到最大值

$$s^{117}(138)=179931895322=2\cdot61\cdot929\cdot1587569$$

之后,该序列终止于 $s^{177}(138)=1$.下一个仍有怀疑的数是 276. Lehmer 对它作了大量计算,后来在得到 Godwin, Selfridge, Wunderlich 以及其他人的帮助,把计算推进到 $s^{469}(276)$,这些结果曾在第一版中提到过. Thomas Struppeck 将这一项作了分解,并且又进一步计算了两次迭代. Andy Guy 写了一个 PARI 程序,从头开始彻夜工作,验证了以前的所有计算,并一直计算到 $s^{487}(276)$.

前途未卜的头几个序列是"Lehmer 的 6 个数",即以 276, 552,564,660,840 以及 966 开始的序列.我们的程序证明了:840 序列取到素数 $s^{746}(840)=601$,并作为一个终止的序列的最大值给出了一个新的记录:

$s^{287}(840)=3463982260143725017429794136098072146586526240388$

$=2^2\cdot 64970467217\cdot 6237379309797547\cdot 2136965558478112990003.$

这一记录最近被 Mitchell Dickerman 打破，他发现 1248 序列的长度为 1075 项，取到的最大值为

$s^{583}(1248)=1231\ 636691\ 923602\ 991963\ 829388\ 638861\ 714770\ 651073\ 275257\ 065104=2^4p$

(有 58 位). 他还将 276 序列算到第 628 项，该项有 65 位数字. Godwin 研究了起始数在 1000 和 2000 之间的 14 个主要的序列，其结果尚不知晓，但发现序列 1848 是终止的. 我们发现以 2580，2850，4488，4830，6792，7752，8862 以及 9540 开始的序列也都是终止的序列.

H. W. Lenstra 证明了：能造出任意长的单调增加的真因子序列. 见 B41 中提到的由 4 个人合写的那篇论文. 下述参考文献中的最后一篇有与数论函数迭代有关的 60 篇文献目录.

参考文献

Jack Alanen, Empirical study of aliquot series, *Math. Rep.*, **133** Stichting Math. Centrum Amsterdam, 1972; see *Math. Comput.*, **28**(1974) 878–880.

E. Catalan, Propositions et questions diverses, *Bull. Soc. Math. France*, **16** (1887–88) 128–129.

John Stanley Devitt, Aliquot Sequences, MSc thesis, The Univ. of Calgary, 1976; see *Math. Comput.*, **32**(1978) 942–943.

J. S. Devitt, R. K. Guy & J. L. Selfridge, Third report on aliquot sequences, *Congr. Numer.* XVIII, Proc. 6th Manitoba Conf. Numer. Math., 1976, 177–204; *MR* **80d**:10001.

L. E. Dickson, Theorems and tables on the sum of the divisors of a number, *Quart. J. Math.*, **44**(1913) 264–296.

Paul Erdős, On asymptotic properties of aliquot sequences, *Math. Comput.*, **30**(1976) 641–645.

Andrew W. P. Guy & Richard K. Guy, A record aliquot sequence, in *Mathematics of Computation 1943–1993* (Vancouver, 1993), *Proc. Sympos. Appl. Math.*, (1994) Amer. Math. Soc., Providence RI, 1984.

Richard K. Guy, Aliquot sequences, in *Number Theory and Algebra*, Academic Press, 1977, 111–118; *MR* **57** #223; *Zbl.* **367**.10007.

Richard K. Guy & J. L. Selfridge, Interim report on aliquot sequences, *Congr. Numer.* V, Proc. Conf. Numer. Math., Winnipeg, 1971, 557–580; *MR* **49** #194; *Zbl.* **266**.10006.

Richard K. Guy & J. L. Selfridge, Combined report on aliquot sequences, The Univ. of Calgary Math. Res. Rep. **225**(May, 1974).

Richard K. Guy & J. L. Selfridge, What drives an aliquot sequence? *Math. Comput.*, **29**(1975) 101–107; *MR* **52** #5542; *Zbl.* **296**.10007. Corrigendum, *ibid.*, **34**(1980) 319–321; *MR* **81f**:10008; *Zbl.* **423**.10005.

Richard K. Guy & M. R. Williams, Aliquot sequences near 10^{12}, *Congr. Numer.* XII, Proc. 4th Manitoba Conf. Numer. Math., 1974, 387–406; *MR* **52** #242; *Zbl.* **359**.10007.

Richard K. Guy, D. H. Lehmer, J. L. Selfridge & M. C. Wunderlich, Second report on aliquot sequences, *Congr. Numer.* IX, Proc. 3rd Manitoba Conf. Numer. Math., 1973, 357–368; *MR* **50** #4455; *Zbl.* **325**.10007.

H. W. Lenstra, Problem 6064, *Amer. Math. Monthly*, **82**(1975) 1016; solution **84** (1977) 580.

G. Aaron Paxson, Aliquot sequences (preliminary report), *Amer. Math. Monthly*, **63**(1956) 614. See also *Math. Comput.*, **26** (1972) 807–809.

P. Poulet, La chasse aux nombres, Fascicule I, Bruxelles, 1929.

P. Poulet, Nouvelles suites arithmétiques, *Sphinx*, Deuxième Année (1932) 53–54.

H. J. J. te Riele, A note on the Catalan-Dickson conjecture, *Math. Comput.*, **27**(1973) 189–192; *MR* **48** #3869; *Zbl.* **255**.10008.

H. J. J. te Riele, Iteration of number theoretic functions, Report NN 30/83, Math. Centrum, Amsterdam, 1983.

B7. 真因子圈或交际数

Poulet 发现了两个数圈，这说明除了 1 和 2 以外，$s^k(n)$还可以有周期 5 和 28. 对 $k\equiv0,1,2,3,4 \bmod 5$，$s^k(12496)$取值

$$12496=2^4\cdot11\cdot71,\quad 14288=2^4\cdot19\cdot47,\quad 15472=2^4\cdot967,$$
$$14536=2^3\cdot23\cdot79,\quad 14264=2^3\cdot1783.$$

对 $k\equiv0,1,\cdots,27 \bmod 28$，$s^k(14316)$取值

14316	19116	31704	47616	83328	177792	295488
629072	589786	294896	358336	418904	366556	274924
275444	243760	376736	381028	285778	152990	122410
97946	48976	45946	22976	22744	19916	17716.

在停滞 50 多年之后，由于高速计算机的出现，Henri Cohen 发现了 9 个周期为 4 的圈，Borho, David 以及 Root 也有一些发现. 最近，D. Moews 和 P. C. Moews 对最大元素小于 10^{10}的这种圈做了彻底的搜索，一共找到 24 个圈，每个圈中最小的数是

1264460	7169104	46722700	330003580	2387776550	4424606020
2115324	18048976	81128632	498215416	2717495235	4823923384
2784580	18656380	174277820	1236402232	2879697304	5373457070
4938136	28158165	209524210	1799281330	3705771825	8653956136.

D. Moews 和 P. C. Moews 给出 5 个大的 4-圈，在 1990 年 9 月 1 日的一封信中，又给出另一个大的 4-圈，其中最小的数是

$$2^6 \cdot 79 \cdot 1913 \cdot 226691 \cdot 207722852483.$$

他们还发现了一个 8-圈：

1095447416　1259477224　1156962296　1330251784
1221976136　1127671864　1245926216　1213138984.

Ren Yuanhua 也发现了 3 个 4-圈，Achim Flammenkamp 同样发现了许多这样的圈，同时他还发现了第二个 8-圈：

1276254780　2299401444　3071310364　2303482780
2629903076　2209210588　2223459332　1697298124

和一个 9-圈：

805984760　1268997640　1803863720　2308845400　3059220620
3367978564　2525983930　2301481286　1611969514.

D. Moews 和 P. C. Moews 继续作穷举搜索，以图找出长度任意、其中最大数的前一元素小于 $3.6 \cdot 10^{10}$ 的所有的圈. 在此范围内还有 3 个 4-圈，它们的最小元素是

15837081520　17616303220　21669628904，

还有一个所有元素均为奇数的 6-圈：

$21548919483 = 3^5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 19 \cdot 431,$

$23625285957 = 3^5 \cdot 7^2 \cdot 13 \cdot 19 \cdot 29 \cdot 277,$

$24825443643 = 3^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19 \cdot 20719,$

$26762383557 = 3^4 \cdot 7^2 \cdot 13 \cdot 19 \cdot 27299,$

$25958284443 = 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot 167 \cdot 1427,$

$23816997477 = 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot 218651.$

人们猜想没有 3-圈. 另一方面，又猜想对每个 k 有无穷多个 k-圈.

参考文献

Walter Borho, Über die Fixpunkte der k-fach iterierten Teilersummenfunktion, *Mitt. Math. Gesellsch. Hamburg*, **9**(1969) 34–48; *MR* **40** #7189.

Achim Flammenkamp, New sociable numbers, *Math. Comput.*, **56**(1991) 871–873.

David Moews & Paul C. Moews, A search for aliquot cycles below 10^{10}, *Math. Comput.*, **57**(1991) 849–855; *MR* **92e**:11151.

David Moews & Paul C. Moews, A search for aliquot cycles and amicable pairs, *Math. Comput.*, **61**(1993) 935–938.

B8. 单真因子序列

真因子序列和真因子圈的思想可以应用于仅对单因子求和的情形,从而产生所谓的单真因子序列(unitary aliquot sequence)和单交际数(unitary sociable number).当考虑的仅仅是对单因子求和时,就用 $\sigma^*(n)$和 $s^*(n)$来取代对应的函数 $\sigma(n)$和 $s(n)$(与 B3 比较).

是否存在无界的单真因子序列? 对此作出估计要比在通常真因子序列的情形有更高的技巧. 仅有的值得认真考虑的序列是包含 6 的奇倍数的序列,6 既是一个单完全数,也是一个通常的完全数.如果 $3 \| n$,序列趋于增加,但当存在 3 的高次幂时,序列将减小,何种情形将起主导作用则是值得研究的问题.一旦序列有一项是 $6m$(m 为奇数),那么 $\sigma^*(6m)$就是 6 的偶倍数,而 $s^*(6m)$则再次是 6 的奇倍数(除了在 m 是 4 的某个奇次幂这种极端罕见的情形之外).

te Riele 致力于寻求 $n<10^5$ 的所有单真因子序列.仅有的一个不终止的也即变成周期性循环的序列是 89610.此后的计算表明,它在第 568 项达到最大值

$$645\,856907\,610421\,353834=2\cdot3^2\cdot13\cdot19\cdot73\cdot653\cdot3047409443791,$$

并终止于第 1129 项.

不到你所期待的素因子个数很大的时候,很难指望会有典型的性状出现.因为这个数有 $\ln\ln n$ 这么大,这种序列常会超出计算

机的能力范围.对接近10^{12}的 80 个序列作检查发现,所有序列都终止或变成周期性循环的,其中有一个序列超过了10^{23}.

单亲和数对和单交际数可能比它们的通常的对应物(指亲和数对和交际数——译者注)出现得更加频繁. Lal, Tiller 和 Summers 发现了周期为 1,2,3,4,5,6,14,25,39 以及 65 的圈.单亲和数对的例子是(56430,64530)和(1080150,1291050),而(30,42,54)是一个 3-圈,(1482,1878,1890,2142,2178)是一个 5-圈.

Cohen(有关定义和文献见 B3)找到了 62 个无穷元亲和数对,每一对中较小的数均小于一百万,以及 8 个阶为 4 的无穷元真因子圈和 3 个阶为 6 的无穷元真因子圈.其他像这样阶小于 17 且最小元素小于一百万的仅有的圈是周期为 11 的圈:

448800, 696864, 1124448, 1651584, 3636096, 6608784
5729136, 3736464, 2187696, 1572432, 895152.

David Penney 和 Carl Pomerance 提出一种可能是无界的真因子序列,它基于 Dedekind 函数(见 B41).

Erdös 在寻找其迭代可能有界的数论函数时,建议定义 $w(n)=n\sum 1/p_i^{a_i}$,其中 $n=\prod p_i^{a_i}$,而 $W^k(n)=w(w^{k-1}(n))$.注意到 $w(n)\perp n$.是否可以证明 $w^k(n)$, $k=1,2,\cdots$是有界的呢? 是否有 $|\{w(n):1\leqslant n\leqslant x\}|=o(x)$?

Erdös 和 Selfridge 称 n 为一个数论函数 $f(m)$ 的**障界**(barrier),如果对所有 $m<n$ 有 $m+f(m)\leqslant n$. Eulerφ 函数(见 B36)和函数 $\sigma(m)$ 增长得太快,因而不可能有障界,但是 $\omega(m)$ 有无穷多个障界吗? 数 2,3,4,5,6,8,9,10,12,14,17,18,20,24,26,28,30,…都是 $\omega(m)$ 的障界. $\Omega(m)$ 有无穷多个障界吗? Selfridge 注意到 99840 是 $\Omega(m)$ 的小于 10^5 的最大的障界. Ma̧kowski 发现,对每个函数而言,$n=1$ 都是一个障界,对每个满足 $f(1)=1$ 的函数 $f(n)$ 来说,2 都是一个障界;特别地,对 m 的因子个数 $d(m)$ 亦然.不等式

$$\max\{d(n-1)+n-1, d(n-2)+n-2\}\geqslant n+2$$

对 $n\geqslant 7$ 成立,对 $n=6$ 不成立.但对 $n\geqslant 3$ 有 $d(n-1)+n-1\geqslant$

$n+1$,故 $d(m)$没有$\geqslant 3$ 的障界.

$$\max_{m<n}(m+d(m))=n+2$$

是否有无穷多个解？这是很值得怀疑的.它有一个解是 $n=24$,下一个更大的解可能要超出计算机的能力范围.

参考文献

Paul Erdős, A mélange of simply posed conjectures with frustratingly elusive solutions, *Math. Mag.*, **52**(1979) 67–70.

P. Erdős, Problems and results in number theory and graph theory, *Congressus Numerantium* **27**, Proc. 9th Manitoba Conf. Numerical Math. Comput., 1979, 3–21.

Richard K. Guy & Marvin C. Wunderlich, Computing unitary aliquot sequences – a preliminary report, *Congressus Numerantium* **27**, Proc. 9th Manitoba Conf. Numerical Math. Comput., 1979, 257–270.

P. Hagis, Unitary amicable numbers, *Math. Comput.*, **25**(1971) 915–918; *MR* **45** #8599.

Peter Hagis, Unitary hyperperfect numbers, *Math. Comput.*, **36**(1981) 299–301.

M. Lal, G. Tiller & T. Summers, Unitary sociable numbers, *Congressus Numerantium* **7**, Proc. 2nd Manitoba Conf. Numerical Math., 1972, 211–216: *MR* **50** #4471.

H. J. J. te Riele, *Unitary Aliquot Sequences*, MR139/72, Mathematisch Centrum, Amsterdam, 1972; reviewed *Math. Comput.*, **32**(1978) 944–945; *Zbl.* 251. 10008.

H. J. J. te Riele, *Further Results on Unitary Aliquot Sequences*, NW12/73, Mathematisch Centrum, Amsterdam, 1973; reviewed *Math. Comput.*, **32**(1978) 945.

H. J. J. te Riele, *A Theoretical and Computational Study of Generalized Aliquot Sequences*, MCT72, Mathematisch Centrum, Amsterdam, 1976; reviewed *Math. Comput.*, **32**(1978) 945–946; *MR* **58** #27716.

C. R. Wall, Topics related to the sum of unitary divisors of an integer, PhD thesis, Univ. of Tennessee, 1970.

B9. 超完全数

Suryanarayana 用 $\sigma^2(n)=2n$ 也即 $\sigma(\sigma(n))=2n$ 来定义超完全数(superperfect number)n.他和 Kanold 证明了:偶的超完全数恰是形如 2^{p-1}的数,这里 2^p-1 是一个 Mersenne 素数.是否有奇的超完全数？若有,Kanold 证明了它们必为完全平方,而 Dandepat 和其他人则证明了:n 或者 $\sigma(n)$至少可被三个不同的素数整除.

更一般地，Bode 定义 m-超完全数(m-superperfect number)是满足 $\sigma^m(n)=2n$ 的整数n.他证明了：对 $m\geqslant 3$，没有偶的 m-超完全数存在.他还证明了，对 $m=2$ 没有小于 10^{10}的超完全数存在.Hunsucker 和 Pomerance 把这个界提高到7×10^{24}.如果 n 是超完全数，则对 n 以及$\sigma(n)$的不同素因子个数，他们还有一些未发表的结果.

如果 $\sigma^2(n)=2n+1$，把 n 称为拟超完全数与较早所用的术语是一致的.Mersenne 素数正是这样的数. 那么，还有其他的拟超完全数吗？是否有满足 $\sigma^2(n)=2n-1$ 的"殆超完全数"存在？

Erdös 问：当 $k\to\infty$时$(\sigma^k(n))^{1/k}$是否有极限？他猜想对每个$n>1$ 极限均为无限.

Schinzel 问：对每个 k，当 $n\to\infty$时是否有 $\lim\inf\sigma^k(n)/n<\infty$？他注意到，对 $k=2$ 这一结论可以由 Rényi 的一个深刻的定理得出.Mąkowski 和 Schinzel 对 $k=2$ 时极限为 1 给出一个初等证明.Helmut Maier 则用筛法证明了 $k=3$ 的结果.

参考文献

Dieter Bode, Über eine Verallgemeinerung der volkommenen Zahlen, Dissertation, Braunschweig, 1971.

P. Erdős, Some remarks on the iterates of the ϕ and σ functions, *Colloq. Math.*, **17**(1967) 195–202.

J. L. Hunsucker & C. Pomerance, There are no odd super perfect numbers less than $7\cdot 10^{24}$, *Indian J. Math.*, **17**(1975) 107–120; *MR* **82b**:10010.

H.-J. Kanold, Über "Super perfect numbers," *Elem. Math.*, **24**(1969) 61–62; *MR* **39** #5463.

Graham Lord, Even perfect and superperfect numbers, *Elem. Math.*, **30** (1975) 87–88.

Helmut Maier, On the third iterates of the ϕ- and σ-functions, *Colloq. Math.*, **49**(1984) 123–130.

Andrzej Mąkowski, On two conjectures of Schinzel, *Elem. Math.*, **31**(1976) 140–141.

A. Mąkowski & A. Schinzel, On the functions $\phi(n)$ and $\sigma(n)$, *Colloq. Math.*, **13**(1964-65) 95–99.

A. Schinzel, Ungelöste Probleme Nr. 30, *Elem. Math.*, **14**(1959) 60–61.

D. Suryanarayana, Super perfect numbers, *Elem. Math.*, **24**(1969) 16–17; *MR* **39** #5706.

D. Suryanarayana, There is no superperfect number of the form $p^{2\alpha}$, *Elem. Math.*, **28**(1973) 148–150; *MR* **48** #8374.

B10. 不 可 及 数

Erdös 证明了,存在无穷多个 n 使 $s(x)=n$ 无解. Alanen 称这样的数 n 为不可及数(untouchable). 事实上 Erdös 证明了不可及数有正的下密度. 下面是小于 100 的不可及数:

2	5	52	88	96	120	124	146	162	178	188	206	210	216	238	246
248	262	268	276	288	290	292	304	306	322	324	326	336	342	372	406
408	426	430	448	472	474	498	516	518	520	530	540	552	556	562	576
584	612	624	626	628	658	668	670	714	718	726	732	738	748	750	756
766	768	782	784	792	802	804	818	836	848	852	872	892	894	896	898
902	916	926	936	964	966	976	982	996							

由于 Goldbach 猜想(C1)的合理性,很可能 5 是惟一的奇不可及数,这是因为如果 $2n+1=p+q+1$(p 和 q 是素数),那么就有 $s(pq)=2n+1$. 这是否可以独立地加以证明呢? 是否有任意长的由不可及数组成的相邻偶数序列? 不可及数之间的间隙到底有多大?

参 考 文 献

P. Erdős, Über die Zahlen der Form $\sigma(n)-n$ und $n-\phi(n)$, *Elem. Math.*, **28**(1973) 83–86; *MR* **49** #2502.

Paul Erdős, Some unconventional problems in number theory, *Astérisque*, **61** (1979) 73–82; *MR* **81h**:10001.

B11. $m\sigma(m)=n\sigma(n)$的解

Leo Moser 注意到: $n\varphi(n)$可以惟一决定 n, 而 $n\sigma(n)$则不行(这里 $\varphi(n)$为 Eulerφ 函数, 见 B36). 例如, 对 $m=12$ 和 $n=14$ 有 $m\sigma(m)=n\sigma(n)$. $\sigma(n)$的积性保证了它有无穷多个解 $m=12q$, $n=14q$, 其中 $q\perp 42$. 于是 Moser 问: 此方程是否有无穷多个本原

解? 所谓本原解,是指对任何 $m^* = m/d, n^* = n/d (d>1)$, (m^*, n^*)都不再是它的解.我们给出的例子是集合 $m = 2^{p-1}(2^q - 1)$, $n = 2^{q-1}(2^p - 1)$中最小的解,这里 $2^p - 1$ 和 $2^q - 1$ 是不同的 Mersenne 素数,从而仅有有限多个解是已知的.另外一组解是 $m = 2^7 \cdot 3^2 \cdot 5^2 \cdot (2^p - 1)$和 $n = 2^{p-1} \cdot 5^3 \cdot 17 \cdot 31$,其中 $2^p - 1$ 是除去 3 和 31 以外的 Mersenne 素数.又在消去公因子 31 之后,$p = 5$ 给出一个本原解.还有其他的解,如 $m = 2^4 \cdot 3 \cdot 5^3 \cdot 7$ 和 $n = 2^{11} \cdot 5^2$ 以及 $m = 2^9 \cdot 5$ 和 $n = 2^3 \cdot 11 \cdot 31$.满足 $m \perp n$ 的解的一个例子是$m = 2^5 \cdot 5$ 和 $n = 3^3 \cdot 7$.如果 $m\sigma(m) = n\sigma(n)$, m/n 有界吗?

Erdös 注意到,如果 n 无平方因子,那么形如 $n\sigma(n)$的整数是不同的.他还可以证明:方程 $m\sigma(m) = n\sigma(n)$的满足 $m < n < x$ 的解数为 $cx + o(x)$.在回答是否有 3 个不同的数 l, m, n 使有 $l\sigma(l) = m\sigma(m) = n\sigma(n)$成立这一问题时,Mąkowski 发现,对不同的 Mersenne 素数 M_{p_i} $(1 \leqslant i \leqslant s)$我们有:$n_i\sigma(n_i)$对 $n_i = A/M_{p_i}$ 取常数值,其中 $A = \prod_{j=1}^{s} M_{p_j}$.方程 $\sigma(a)/a = \sigma(b)/b$ 是否有无穷多个本原解? 若不限制解是本原的,Erdös 可以证明此方程满足 $a < b < x$ 的解数至少是$cx + o(x)$;若加上限制条件 $a \perp b$,则其解还一个都不知道.

Erdös 相信,对每个 $\varepsilon > 0$, $x\sigma(x) = n$ 的解数小于 $n^{\varepsilon/\ln\ln n}$,他说此解数可能小于$(\ln n)^c$.

参考文献

P. Erdős, Remarks on number theory II: some problems on the σ function, *Acta Arith.*, **5**(1959) 171–177; *MR* **21** #6348.

B12. $d(n)$和 $\sigma_k(n)$的相似物

可以用 $\sigma_k(n)$代替 $\sigma(n)$来提出类似的问题,这里 $\sigma_k(n)$是 n 的因子的 k 次幂之和.例如,是否有不同的数 m 和 n 使得有

$m\sigma_2(m)=n\sigma_2(n)$? 当 $k=0$ 时,对 $(m,n)=(18,27),(24,32),(56,64),(192,224)$ 有 $md(m)=nd(n)$. 在最后这对数中补上 168,就得到三个不同的数使 $ld(l)=md(m)=nd(n)$ 成立. 有形如

$$m = 2^{qt-1}p, \qquad n = 2^{pt\cdot 2^{tu}-1}q$$

的本原解 (m,n),其中 p 和 $q=u+p\cdot 2^{tu}$ 为素数,但不能直接得出这样的解有无穷多个. 还可以造出许多其他的解,例如 $(2^{70},2^{63}\cdot 71)$, $(3^{19},3^{17}\cdot 5)$ 以及 $(5^{51},5^{49}\cdot 13)$.

Bencze 证明了不等式

$$\frac{n^k+1}{2} \geqslant \frac{\sigma_k(n)}{\sigma_{k-l}(n)} \geqslant \sqrt{n^l} \qquad (对 0 \leqslant l \leqslant k),$$

并给出了不少于 60 个应用.

参考文献

Mihály Bencze, A contest problem and its application (Hungarian), *Mat. Lapok Ifjúsági Folyóirat (Románia)*, **91**(1986) 179–186.

B13. $\sigma(n)=\sigma(n+1)$ 的解

Sierpiński 问是否无穷多次有 $\sigma(n)=\sigma(n+1)$ 成立? Hunsucker, Nebb 和 Stearns 扩大了 Mąkowski 以及 Mientka 和 Vogt 的表,他们在小于 10^7 的范围内发现它恰有 113 个解

$$14, 206, 957, 1334, 1364, 1634, 2685, 2974, 4364, \cdots.$$

他们还对方程 $\sigma(n)=\sigma(n+l)$ 得到统计的结果;对此 Mientka 和 Vogt 曾问道:对何种 l(如果有这种 l 存在的话)有无穷多个解? 如果 l 是一个阶乘,他们找到了许多个解,但对 $l=15$ 和 $l=69$,只找到两个解. 他们又问:对每个 l 和 m,是否都存在 n 使得有 $\sigma(n)+m=\sigma(n+l)$ 成立?

对 $\sigma_k(n)$ 可以问相应的问题,这里 $\sigma_k(n)$ 是 n 的因子的 k 次幂之和(对 $k=0$ 见 B15). 方程 $\sigma_2(n)=\sigma_2(n+1)$ 惟一的解是 $n=6$,这是因为 $\sigma_2(2n)>\sigma_2(2n+1)$(对 $n>7$)且 $\sigma_2(2n)>5n^2>$

$(\pi^2/8)(2n-1)^2 > \sigma_2(2n-1)$. 注意到有 $\sigma_2(24)=\sigma_2(26)$，而 Erdös则怀疑 $\sigma_2(n)=\sigma_2(n+2)$是否能有无穷多个解，他认为 $\sigma_3(n)=\sigma_3(n+2)$根本没有解.

参考文献

Richard K. Guy & Daniel Shanks, A constructed solution of $\sigma(n)=\sigma(n+1)$, *Fibonacci Quart.*, **12**(1974) 299; *MR* **50** #219.

John L. Hunsucker, Jack Nebb & Robert E. Stearns, Computational results concerning some equations involving $\sigma(n)$, *Math. Student*, **41**(1973) 285–289.

W. E. Mientka & R. L. Vogt, Computational results relating to problems concerning $\sigma(n)$, *Mat. Vesnik*, **7**(1970) 35–36.

B14. 某些无理级数

$\sum_{n=1}^{\infty}(\sigma_k(n)/n!)$ 是无理数吗? 对 $k=1$ 和 2 这是对的.

Erdös 证明了级数

$$\sum_{n=1}^{\infty}\frac{1}{2^n-1}=\sum_{n=1}^{\infty}\frac{d(n)}{2^n}$$

的无理性，而 Peter 和 Borwein 则证明了：如果 q 是一个异于 0，± 1的整数，而 r 是一个异于 0 及 $-q^n$ 的有理数，则

$$\sum_{n=1}^{\infty}\frac{1}{q^n+r} \quad 和 \quad \sum_{n=1}^{\infty}\frac{(-1)^n}{q^n+r}$$

是无理数.

参考文献

Peter B. Borwein, On the irrationality of $\sum 1/(q^n+r)$, *J. Number Theory*, **37**(1991) 253–259.

Peter B. Borwein, On the irrationality of certain series, *Math. Proc. Cambridge Philos. Soc.*, **112**(1992) 141–146; *MR* **93g**:11074.

P. Erdős, On arithmetical properties of Lambert series, *J. Indian Math. Soc.(N.S.)* **12**(1948) 63–66.

P. Erdős, On the irrationality of certain series: problems and results, in *New Advances in Transcendence Theory*, Cambridge Univ. Press, 1988, pp. 102–109.

P. Erdős & M. Kac, Problem 4518, *Amer. Math. Monthly*, **60**(1953) 47. Solution R. Breusch, **61**(1954) 264–265.

B15. $\sigma(q)+\sigma(r)=\sigma(q+r)$的解

Max Rumney(见 *Eureka*, 26(1963) 12)问道:方程 $\sigma(q)+\sigma(r)=\sigma(q+r)$是否有无穷多个本原的解(本原的含义与 B11 中所用的定义类似)? 若 $q+r$ 为素数,则仅有的解是$(q,r)=(1,2)$.若 $q+r=p^2$(这里 p 为素数),则 q 和 r 中必有一个(比方说是 q)是素数,且有 $r=2^nk^2$(这里 $n\geqslant 1$ 且 k 为奇数).如果 $k=1$,那么当 $p=2^n-1$ 是一个 Mersenne 素数而 $q=p^2-2^n$ 是一个素数时方程有一个解;对 $n=2,3,5,7,13$ 和 19 亦然.对 $k=3$ 没有解,对 $k=5$ 及 $n<189$ 也没有解.对 $k=7,n=1$ 和 3 给出解$(q,r,q+r)=(5231,2\cdot 7^2,73^2)$和$(213977,2^3\cdot 7^2,463^2)$.其他的解是$(k,n)=(11,1),(11,3),(19,5),(25,1),(25,9),(49,9),(53,1),(97,5),(107,5),(131,5),(137,1),(149,5),(257,5),(277,1),(313,3)$和$(421,3)$.满足 $q+r=p^3$ 且 p 为素数的解是$\sigma(2)+\sigma(6)=\sigma(8)$和

$$\sigma(11638687)+\sigma(2^2\cdot 13\cdot 1123)=\sigma(227^3).$$

Erdös 问:有多少个满足 $q+r<x$ 的(不一定本原的)解? 此解数是 $cx+o(x)$呢还是有更高的阶? 如果 $s_1<s_2<\cdots$是一组数,它们使得 $\sigma(s_i)=\sigma(q)+\sigma(s_i-q)$有一个适合 $q<s_i$ 的解,那么序列$\{s_i\}$的密度是什么?

参 考 文 献

M. Sugunamma, PhD thesis, Sri Venkataswara Univ., 1969.

B16. 幂　　数

Erdös 和 Szekeres 研究了这样的数 n:若素数 p 整除 n,则 p^i 也整除 n,这里 i 是一个给定的大于 1 的数. Golomb 给这样的数取名为幂数(powerful)并展示出有无穷多对相邻的幂数. 在回答

他的“6 不可表为两个幂数之差”这一猜想时，Władysław Narkiewicz 注意到有 $6=5^4 7^3-463^2$，且有无穷多种这样的表法．事实上 1971 年 Richard P. Stanley 曾用 Pell 方程的理论证明了(未发表)：每个非零整数都是两个幂数之差，1 是两个非平方的幂数之差，且二者均有无穷多种表法．

Erdös 用 $u_1^{(k)}<u_2^{(k)}<\cdots$ 表示其素因子的幂均 $\geqslant k$ 的整数，有时称之为 k -幂数(k-full number)．他问：方程 $u_{i+1}^{(2)}-u_i^{(2)}=1$ 是否有无穷多个并非来自 Pell 方程 $x^2-dy^2=\pm 1$ 解？是否有常数 c 存在，使该方程满足 $u_i<x$ 的解数小于 $(\ln x)^c$？ $u_{i+1}^{(3)}-u_i^{(3)}=1$ 没有解吗？方程 $u_{i+2}^{(2)}-u_{i+1}^{(2)}=1$ 与 $u_{i+1}^{(2)}-u_i^{(2)}=1$ 没有联立解吗？另外还有一些其他的问题，其中有些问题已由 Mąkowski 予以回答．

例如，Mąkowski 注意到，$7^3x^2-3^3y^2=1$ 有无穷多个解，这并非是通常视为 Pell 方程所得到的．他还注意到，

$$(2^{k+1}-1)^k,\quad 2^k(2^{k+1}-1)^k,\quad (2^{k+1}-1)^{k+1}$$

是算术级数中的 k -幂数；又若 $a_1,a_2,\cdots,a_s$ 是一个算术级数中的 k -幂数，公差为 d，那么

$$a_1(a_s+d)^k,a_2(a_s+d)^k,\cdots,a_s(a_s+d)^k,(a_s+d)^{k+1}$$

也是 $s+1$ 个这样的数．由于

$$a^k(a^l+\cdots+1)^k+a^{k+1}(a^l+\cdots+1)^k+\cdots+a^{k+l}(a^l+\cdots+1)^k$$
$$=a^k(a^l+\cdots+1)^{k+1},$$

从而 $l+1$ 个 k -幂数之和能是一个 k -幂数．他说，当要求诸数互素时，上面最后两个问题就变得困难了．然而，Nitaj 构造出 $x+y=z$ 的三个无穷解族，它们是用互素的 3 -幂数给出的．一个特例是

$$17^3\cdot106219^3+2^7\cdot3^4\cdot5^3\cdot7^3\cdot2287^3=37^3\cdot197^3\cdot307^3.$$

Heath-Brown 证明了，每个充分大的数是三个幂数之和．如果他的猜想“每个充分大的数 $n\equiv 7\bmod 8$ 可用二次型 $x^2+y^2+125z^2$ 表出”能得到证明的话，他的上述证明就可以大大加以简化．Erdös 认为这可以从 Duke 和 Iwaniec 的工作得出：确切地说

可以参看 Moroz 的即将发表的论文.

是否只有有限多个幂数 n 使 n^2-1 也为幂数呢?(见 D2 中 Granville 的文献.)

Gerry Myerson 注意到下述猜想仍未解决:若 p 为奇素数, u 和 v 是满足 $u^2-pv^2=1$ 的最小正整数,那么

$$¿\quad p\nmid v \quad ?$$

对 $p\equiv 1 \bmod 4$ 和 $p<6270713$ 以及对 $p\equiv -1 \bmod 4$ 和 $p<7679299$ 此猜想已获得验证.若 p 不是素数,则此猜想不真. Myerson 相信 46 和 430 是该猜想的两个最小的反例.

参考文献

N. C. Ankeny, E. Artin & S. Chowla, The class-number of real quadratic number fields, *Ann. of Math.*(2), **56**(1952) 479–493; *MR* **14**, 251.

B. D. Beach, H. C. Williams & C. R. Zarnke, Some computer results on units in quadratic and cubic fields, *Proc. 25th Summer Meet. Canad. Math. Congress*, Lakehead, 1971, 609–648; *MR* **49** #2656.

David Drazin & Robert Gilmer, Complements and comments, *Amer. Math. Monthly*, **78**(1971) 1104–1106 (esp. p. 1106).

W. Duke, Hyperbolic distribution problems and half-integral weight Maass forms, *Invent. Math.*, **92**(1988) 73–90; *MR* **89d**:11033.

P. Erdős, Problems and results on consecutive integers, *Eureka*, **38**(1975–76) 3–8.

P. Erdős & G. Szekeres, Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem, *Acta Litt. Sci. Szeged*, **7**(1934) 95–102; *Zbl.* **10**, 294.

S. W. Golomb, Powerful numbers, *Amer. Math. Monthly*, **77**(1970) 848–852; *MR* **42** #1780.

D. R. Heath-Brown, Ternary quadratic forms and sums of three square-full numbers, *Séminaire de Théorie des Nombres, Paris, 1986-87*, Birkhäuser, Boston, 1988; *MR* **91b**:11031.

D. R. Heath-Brown, Sums of three square-full numbers, in Number Theory, I (Budapest, 1987), *Colloq. Math. Soc. János Bolyai*, **51**(1990) 163–171; *MR* **91i**:11036.

D. R. Heath-Brown, Square-full numbers in short intervals, *Math. Proc. Cambridge Philos. Soc.*, **110**(1991) 1–3; *MR* **92c**:11090.

Aleksander Ivić, On the asymptotic formulas for powerful numbers, *Publ. Math. Inst. Beograd (N.S.)*, **23(37)**(1978) 85–94; *MR* **58** #21977.

A. Ivić & P. Shiu, The distribution of powerful integers, *Illinois J. Math.*, **26**(1982) 576–590; *MR* **84a**:10047.

H. Iwaniec, Fourier coefficients of modular forms of half-integral weight, *Invent.*

Math., **87**(1987) 385–401; *MR* **88b**:11024.
C.-H. Jia, On square-full numbers in short intervals, *Acta Math. Sinica* (*N.S.*) **5**(1987) 614–621.
Liu Hong-Quan, On square-full numbers in short intervals, *Acta Math. Sinica* (*N.S.*), **6**(1990) 148–164; *MR* **91g**:11105.
Andrzej Mąkowski, On a problem of Golomb on powerful numbers, *Amer. Math. Monthly*, **79**(1972) 761.
Andrzej Mąkowski, Remarks on some problems in the elementary theory of numbers, *Acta Math. Univ. Comenian.*, **50/51**(1987) 277–281; *MR* **90e**:11022.
Wayne L. McDaniel, Representations of every integer as the difference of powerful numbers, *Fibonacci Quart.*, **20**(1982) 85–87.
Richard A. Mollin, The power of powerful numbers, *Internat. J. Math. Math. Sci.*, **10**(1987) 125–130; *MR* **88e**:11008.
Richard A. Mollin & P. Gary Walsh, On non-square powerful numbers, *Fibonacci Quart.*, **25**(1987) 34–37; *MR* **88f**:11006.
Richard A. Mollin & P. Gary Walsh, On powerful numbers, *Internat. J. Math. Math. Sci.*, **9**(1986) 801–806; *MR* **88f**:11005.
Richard A. Mollin & P. Gary Walsh, A note on powerful numbers, quadratic fields and the Pellian, *CR Math. Rep. Acad. Sci. Canada*, **8**(1986) 109–114; *MR* **87g**:11020.
Richard A. Mollin & P. Gary Walsh, Proper differences of non-square powerful numbers, *CR Math. Rep. Acad. Sci. Canada*, **10**(1988) 71–76; *MR* **89e**:11003.
L. J. Mordell, On a pellian equation conjecture, *Acta Arith.*, **6**(1960) 137–144; *MR* **22** #9470.
B. Z. Moroz, On representation of large integers by integral ternary positive definite quadratic forms, *Journées Arithmetiques*, Geneva.
Abderrahmane Nitaj, On a conjecture of Erdős on 3-powerful numbers, *London Math. Soc.*, (submitted).
Peter Georg Schmidt, On the number of square-full integers in short intervals, *Acta Arith.*, **50**(1988) 195–201; corrigendum, **54**(1990) 251–254; *MR* **89f**:11131.
W. A. Sentance, Occurrences of consecutive odd powerful numbers, *Amer. Math. Monthly*, **88**(1981) 272–274.
P. Shiu, On square-full integers in a short interval, *Glasgow Math. J.*, **25** (1984) 127–134.
P. Shiu, The distribution of cube-full numbers, *Glasgow Math. J.*, **33**(1991) 287–295. *MR* **92g**:11091.
P. Shiu, Cube-full numbers in short intervals, *Math. Proc. Cambridge Philos. Soc.*, **112** (1992) 1–5; *MR* **93d**:11097.
A. J. Stephens & H. C. Williams, Some computational results on a problem concerning powerful numbers, *Math. Comput.*, **50**(1988) 619–632.
D. Suryanarayana, On the distribution of some generalized square-full integers, *Pacific J. Math.*, **72**(1977) 547–555; *MR* **56** #11933.
D. Suryanarayana & R. Sitaramachandra Rao, The distribution of square-full integers. *Ark. Mat.*. **11**(1973) 195–201: *MR* **49** #8948.
Charles Vanden Eynden, Differences between squares and powerful numbers,

*816-11-305, *Abstracts Amer. Math. Soc.*, **6**(1985) 20.
David T. Walker, Consecutive integer pairs of powerful numbers and related Diophantine equations, *Fibonacci Quart.*, **14**(1976) 111–116; *MR* **53** #13107.
Yuan Ping-Zhi, On a conjecture of Golomb on powerful numbers (Chinese. English summary), *J. Math. Res. Exposition*, **9**(1989) 453–456; *MR* **91c**:11009.

B17. 指数完全数

设 $n=p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$,如果 $d\mid n$,$d=p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}$,其中 $b_j\mid a_j(1\leqslant j\leqslant r)$,则 Straus 和 Subbarao 称 d 为 n 的一个指数因子(exponential divisor)(e-因子).如果 $\sigma_e(n)=2n$,他们就把 n 称为是一个 e-完全数(e-perfect),这里 $\sigma_e(n)$是 n 的 e-因子之和.e-完全数的一些例子是

$$2^2\cdot3^2, 2^2\cdot3^3\cdot5^2, 2^3\cdot3^2\cdot5^2, 2^4\cdot3^2\cdot11^2, 2^4\cdot3^3\cdot5^2\cdot11^2,$$
$$2^6\cdot3^2\cdot7^2\cdot13^2, 2^6\cdot3^3\cdot5^2\cdot7^2\cdot13^2, 2^7\cdot3^2\cdot5^2\cdot7^2\cdot13^2,$$
$$2^8\cdot3^2\cdot5^2\cdot7^2\cdot139^2$$

以及

$$2^{19}\cdot3^2\cdot5^2\cdot7^2\cdot11^2\cdot13^2\cdot19^2\cdot37^2\cdot79^2\cdot109^2\cdot157^2\cdot313^2.$$

若 m 无平方因子,则 $\sigma_e(m)=m$,于是若 n 为 e-完全数且 m 无平方因子($m\perp n$),那么 mn 为 e-完全数.因此只要考虑幂(B16) e-完全数即可.

Straus 和 Subbarao 证明了没有奇的 e-完全数,事实上不存在奇数 n 使对任何整数 $k>1$ 都成立 $\sigma_e(n)=kn$.他们还证明了:对每个 r,有 r 个素因子的(幂)e-完全数的个数是有限的,且同样的结论对 e-重完全数(e-multiperfect number)依然成立($k>2$).

是否有不被 3 整除的 e-完全数?

Straus 和 Subbarao 猜想:仅有有限多个不被任何给定素数 p 整除的 e-完全数.

是否有 e-重完全数存在?

参考文献

E. G. Straus & M. V. Subbarao, On exponential divisors, *Duke Math. J.*, **41**(1974) 465–471; *MR* **50** #2053.

M. V. Subbarao, On some arithmetic convolutions, *Proc. Conf. Kalamazoo MI, 1971, Springer Lecture Notes in Math.*, **251**(1972) 247–271; *MR* **49** #2510.

M. V. Subbarao & D. Suryanarayana, Exponentially perfect and unitary perfect numbers, *Notices Amer. Math. Soc.*, **18**(1971) 798.

B18. $d(n)=d(n+1)$的解

Claudia Spiro 证明了 $d(n)=d(n+5040)$有无穷多个解,而 Heath-Brown 则用她的思想证明了有无穷多个 n 使$d(n)=d(n+1)$成立,Pinner 将此结果延拓到方程 $d(n)=d(n+a)$(a 为任意给定的整数). 许多例子来自恰为两个不同素数乘积的相邻数对,人们猜想有无穷多个相邻整数组成的三数组 $n,n+1,n+2$,它们均为两个素数之积. 例如,$n=33,85,93,141,201,213,217,301,393,445,633,697,921,\cdots$.显然不可能有四个这样的数,但可能有更长的相邻整数序列,其中每个数有同样多个因子. 例如

$$d(242)=d(243)=d(244)=d(245)=6$$

以及

$$d(40311)=d(40312)=d(40313)=d(40314)=d(40315)=8.$$

这种序列可以有多长? 在一封 1987 年 7 月 16 日的信中, Stephane Vandemergel 给出了 7 个数的序列:$171893=19\cdot83\cdot109$, $171894=2\cdot3\cdot38649$, $171895=5\cdot31\cdot1109$, $171896=2^3\cdot21487$, $171897=3\cdot11\cdot5209$, $171898=2\cdot61\cdot1409$, $171899=7\cdot13\cdot1889$,其中每个数都有 8 个因子. 1990 年, Ivo Düntsch 和 Roger Eggleton 发现了一些这样的 7 个数的序列,两个 8 个数的序列和一个 9 个数的序列, 每个数均有 48 个因子. 最后面这个例子从 17796126877482329126044 开始,可能它不是这种类型的最小的序列.

Erdös 相信,对每个 k,都存在长为 k 的序列,但他看不出怎样

用 n 来给出 k 的上界.

Erdös, Pomerance 和 Sárközy 证明了，在 $n \leqslant x$ 中使 $d(n) = d(n+1)$ 成立的数的个数 $\ll x/(\ln \ln x)^{1/2}$，而 Hildebrand 证明了此数 $\gg x/(\ln \ln x)^3$. 前面三位还证明了在 $n \leqslant x$ 中使比值 $d(n)/d(n+1)$ 处于集合 $\{2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3\}$ 中的数的个数为 $\asymp x/(\ln \ln x)^{1/2}$.

Erdös 证明了：满足 $d(n+1) > d(n)$ 的数 n 的密度是 $\frac{1}{2}$. 这和上述结果结合起来就解决了 S. Chowla 的一个猜想. Fabrykowski 和 Subbarao 将此推广到用 $n+h$ 代替 $n+1$ 的情形.

Erdös 又令

$$1 = d_1 < d_2 < \cdots < d_r = n$$

是 n 的所有因子的集合(按次序排列)，定义

$$f(n) = \sum_1^{r-1} d_i/d_{i+1},$$

并要求我们证明 $\sum_{n=1}^{x} f(n) = (1 + o(1)) x \ln x$.

Erdös 和 Mirsky 希望求得最大的 k，使诸数 $d(n), d(n+1), \cdots, d(n+k)$ 全不相同. 它们仅有平凡的界，这个界大概是 $k = (\ln n)^c$.

参考文献

P. Erdős, Problem P. 307, *Canad. Math. Bull.*, **24**(1981) 252.

P. Erdős & L. Mirsky, The distribution of values of the divisor function $d(n)$, *Proc. London Math. Soc.*(3), **2**(1952) 257–271.

P. Erdős, C. Pomerance & A. Sárközy, On locally repeated values of certain arithmetic functions, II, *Acta Math. Hungarica*, **49**(1987) 251–259; *MR* **88c**:11008.

J. Fabrykowski & M. V. Subbarao, Extension of a result of Erdős concerning the divisor function, *Utilitas Math.*, **38**(1990) 175–181; *MR* **92d**:11101.

D. R. Heath-Brown, A parity problem from sieve theory, *Mathematika*, **29** (1982) 1–6 (esp. p. 6).

D. R. Heath-Brown, The divisor function at consecutive integers, *Mathematika*, **31**(1984) 141–149.

Adolf Hildebrand, The divisors function at consecutive integers, *Pacific J. Math.*, **129** (1987) 307–319; *MR* **88k**:11062.

M. Nair & P. Shiu, On some results of Erdős and Mirsky, *J. London Math. Soc.*(2), **22**(1980) 197–203; and see *ibid.*, **17**(1978) 228–230.

C. Pinner, M.Sc. thesis, Oxford, 1988.

A. Schinzel, Sur un problème concernant le nombre de diviseurs d'un nombre naturel, *Bull. Acad. Polon. Sci. Ser. sci. math. astr. phys.*, **6**(1958) 165–167.

A. Schinzel & W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.*, **4**(1958) 185–208.

W. Sierpiński, Sur une question concernant le nombre de diviseurs premiers d'un nombre naturel, *Colloq. Math.*, **6**(1958) 209–210.

B19. 有相同素因子集的$(m,n+1)$和$(m+1,n)$

Motzkin 和 Straus 要求使 m 和 $n+1$ 有同样的不同素因子集的所有数对 m,n. 对 n 和 $m+1$ 也有类似的问题. 以前人们认为这样的数对必定形如 $m=2^k+1, n=m^2-1(k=0,1,2,\cdots)$, 直到 Conway 发现了 $m=5\cdot7, n+1=5^4\cdot7$, 后来又发现有 $n=2\cdot3^7, m+1=2^2\cdot3^2$, 才知并非如此. 还有别的数对存在吗?

类似地, Erdös 问是否存在异于 $m=2^k-2, n=2^k(2^k-2)$的数 $m,n(m<n)$, 使 m 和 n 有同样的素因子. 类似地, 对 $m+1$ 和 $n+1$ 也有同样的问题. Mąkowski 找到了数对 $m=3\cdot5^2, n=3^5\cdot5$. 对它们有 $m+1=2^2\cdot19, n+1=2^6\cdot19$. 请与问题 B29 比较.

Pomerance 问: 是否有奇数 $n>1$ 使 n 和 $\sigma(n)$有同样的素因子? 他猜想没有.

第一段中的例子 $1+2\cdot3^7=5^4\cdot7$ 因与 ABC 猜想(ABC conjecture)有关而有它自身的意义.

数论中许多经典问题(Goldbach 猜想, 孪生素数, Fermat 问题, Waring 问题, Catalan 猜想)之所以难解, 与乘法和加法之间的冲突有关. 粗略地说, 在三个数之间如果有一个加法关系, 那么它们的素因子不能全都很小.

设 $A+B=C$, 这里 $\gcd(A,B,C)=1$. 定义根 R 为整除 ABC 的最大无平方因子整数, 定义幂 P 为

$$P=\frac{\ln\max(|A|,|B|,|C|)}{\ln R},$$

则对给定的 η 是否仅有有限多个三数组 $\{A,B,C\}$ 适合 $P \geqslant \eta$ 呢? 此猜想的一个更强的形式是 $\limsup P = 1$. 这一猜想的两种形式看来都无望获得解决. 刚刚给的例子是下表中的第五个.

Joe Kanapka(他是 Noam Elkies 的一个学生)做出了满足 $C < 2^{32}$ 和 $P > 1.2$ 的所有例子的表,它们有接近 1000 个,我所知道的头十个是

P	A	B	C	作者
1.629912	2	$3^{10} \cdot 109$	23^5	Reyssat
1.625991	11^2	$3^2 \cdot 5^6 \cdot 7^3$	$2^{21} \cdot 23$	de Weger(D10)
1.623490	$19 \cdot 1307$	$7 \cdot 29^2 \cdot 31^8$	$2^8 \cdot 3^{22} \cdot 5^4$	Browkin-Brzeziński
1.580756	283	$5^{11} \cdot 13^2$	$2^8 \cdot 3^8 \cdot 17^3$	Br-Br, Nitaj
1.567887	1	$2 \cdot 3^7$	$5^4 \cdot 7$	Lehmer(B29)
1.547075	7^3	3^{10}	$2^{11} \cdot 29$	de Weger
1.526999	$13 \cdot 19^6$	$2^{30} \cdot 5$	$3^{13} \cdot 11^2 \cdot 31$	Nitaj
1.502839	239	$5^8 \cdot 17^3$	$2^{10} \cdot 37^4$	Br-Br, Nitaj
1.497621	$5^2 \cdot 7937$	7^{13}	$2^{18} \cdot 3^7 \cdot 13^2$	de Weger
1.492432	$2^2 \cdot 11$	$3^2 \cdot 13^{10} \cdot 17 \cdot 151 \cdot 4423$	$5^9 \cdot 139^6$	Nitaj

Browkin 和 Brzeziński 把 ABC 猜想推广成一个关于有不变为零的子和的互素整数的方程 $a_1 + \cdots + a_n = 0$ 的"n -猜想"(ABC 猜想是它当 $n=3$ 的情形). R 和 P 定义类似. 他们猜想有 $\limsup P = 2n-5$. 他们证明了有 $\limsup P \geqslant 2n-5$,还给出了许多有关 ABC 猜想($P > 1.4$)的例子. 他们的方法是寻求逼近整数之根的有理数(注意,上面最好的例子与 $109^{1/5}$ 能良好逼近 23/9 有关). Abderrahmane Nitaj 用到一个类似的方法,其中的一些结果由 Robert Styer(D10)独立地发现过. Catalan 关系 $1 + 2^3 = 3^2$ 给出一个不大好的值 $P \approx 1.22629$.

ABC 猜想和 Fermat 问题之间的关系见 D2 中 Granville 的文献. 的确,如果 $A = a^p, B = b^p, C = c^p$,且 Fermat 方程 $A + B = C$ 成立,那么椭圆曲线

$$y^2 = x(x-A)(x+B)$$

有判别式 $(4ABC)^2$.

参考文献

Jerzy Browkin & Juliusz Brzeziński, Some remarks on the *abc*-conjecture, *Math. Comput.*, (to appear).

Noam D. Elkies, *ABC* implies Mordell, *Internat. Math. Res. Notices*, **1991** no. 7, 99–109; *MR* **93d**:11064.

Serge Lang, Old and new conjectured diophantine inequalities, *Bull. Amer. Math. Soc.*, **23**(1990) 37–75.

A. Mąkowski, On a problem of Erdős, *Enseignement Math.*(2), **14**(1968) 193.

Abderrahmane Nitaj, 1993 preprint.

András Sárközy, On sums $a+b$ and numbers of the form $ab+1$ with many prime factors, *Österreichisch-Ungarisch-Slowakisches Kolloquium über Zahlentheorie* (Maria Trost, 1992), 141–154, *Grazer Math. Ber.*, **318** Karl-Franzens-Univ. Graz, 1993.

C. L. Stewart & Yu Kun-Rui, On the *abc* conjecture, *Math. Ann.*, **291**(1991) 225–230; *MR* **92k**:11037.

R. Tijdeman, The number of solutions of Diophantine equations, in Number Theory, II (Budapest, 1987), *Colloq. Math. Soc. János Bolyai*, **51**(1990) 671–696.

B20. Cullen 数

人们对 Cullen 数(Cullen number)$n\cdot 2^n+1$ 也一直有某种兴趣,对 $2\leqslant n\leqslant 1000$,除了 $n=141$ 以外,它们都是合数.这可能是强小数定律的一个好的例子,因为 Fermat(小)定理告诉我们:$(p-1)2^{p-1}+1$ 和 $(p-2)2^{p-2}+1$ 二者都能被 p 整除,故而对于小的数 n(其中素数的密度很大),Cullen 数很可能是合数.此外,正如 John Conway 所观察到的:Cullen 数可以被 $2n-1$ 整除,如果它是一个形如 $8k\pm 3$ 的素数.他问 p 和 $p\cdot 2^p+1$ 是否可能同为素数.Wilfrid Keller 注意到 Conway 的发现可推广如下:记 $C_n=n2^n+1$, $W_n=n2^n-1$,那么素数 p 是整除 $C_{(p+1)/2}$ 和 $W_{(3p-1)/2}$,或者是整除 $C_{(3p-1)/2}$ 和 $W_{(p+1)/2}$,要视 Legendre 符号(见 F5)$\left(\frac{2}{p}\right)$ 是等于 -1 还是 $+1$ 而定.Keller 对 $n=4713,5795,6611$ 以及 18496 找到了为素数的 Cullen 数.在 $n\leqslant 30000$ 以内不再有其他为素数的 Cullen 数了.

Riesel 看出对应的数 $n\cdot 2^n-1$ 当 $n=2,3,6,30,75,81,115$ 时为素数. Jönsson 发现当 $n=362$ 时, Keller 发现当 $n=123,249,384,462,512$(即 M_{521}), $751,822,5312,7755,9531,12379,15822,18885$ 时它们均为素数. 这些数中有许多也曾被 Waldemar Gorzkowski 发现过. 在 $n\leqslant 20000$ 以内不再有其他这样的数了. 与上面 Conway 的问题相平行地, Keller 注意到此处 3, 751 和 12379 是素数.

参考文献

Ingemar Jönsson, On certain primes of Mersenne-type, *Nordisk Tidskr. Informationsbehandling* (*BIT*), **12** (1972) 117–118; *MR* **47** #120.

Wilfrid Keller, New Cullen primes, (92-11-20 preprint).

Hans Riesel, *En Bok om Primtal* (Swedish), Lund, 1968; supplement Stockholm, 1977; *MR* **42** #4507, **58** #10681.

B21. 对所有 n 均为合数的数 $k\cdot 2^n+1$

设 $N(x)$ 为不超过 x 且使得对任何正整数 n, $k\cdot 2^n+1$ 都不是素数的奇正整数 k 的个数. Sierpiński 利用覆盖同余式(见 F3)证明了 $N(x)$ 与 x 同时趋向于无穷. 例如, 如果

$$k\equiv 1 \bmod 641\cdot(2^{32}-1) \quad 且\ k\equiv -1 \bmod 6700417,$$

那么序列 $k\cdot 2^n+1$ $(n=0,1,2,\cdots)$ 中每个数都可以被诸素数 3, 5, 17, 257, 641, 65537, 6700417 中恰好一个整除. 他还注意到, 对 k 的某些别的值, 3, 5, 7, 13, 17, 241 中至少有一个数能整除 $k\cdot 2^n+1$.

Erdös 和 Odlyzko 证明了

$$\left(\frac{1}{2}-c_1\right)x\geqslant N(x)\geqslant c_2x.$$

对所有 n 使 $k\cdot 2^n+1$ 都为合数的最小的 k 的值是什么? Selfridge 发现 3, 5, 7, 13, 19, 37, 73 中总有一个数能整除 $78557\cdot 2^n+1$. 他还注意到, 对每个 $k<383$ 都有一个形如 $k\cdot 2^n+1$ 的素数, 而 Hugh Williams 发现了素数 $383\cdot 2^{6393}+1$.

在本书第一版中我们写道:确定最小的 k 现在可能已在计算机的能力范围之内,尽管 Keller 对此表示怀疑. Baillie, Cormack 和 Williams, Keller, Buell 和 Young 等人都做过深入的计算.答案看起来几乎肯定像是 $k=78557$,但还有 35 个数:

4847	5297	5359	7013	10223	13787	19249	21181	22699	24737
25819	27653	27923	28433	33661	34999	39781	44131	46157	46187
46471	47897	48833	50693	54767	55459	59569	60443	60541	63017
65567	67607	69109	74191	74269					

存在下述的可能性:对这些数中任何一个及 $n \leqslant 50000$ 没有一个能使 $k \cdot 2^n+1$ 成为素数.

在 Keller 的第二篇文献中有关本论题的完整综述后面附有很完全的文献目录.

参考文献

Robert Baillie, New primes of the form $k \cdot 2^n+1$, *Math. Comput.*, **33**(1979) 1333–1336; *MR* **80h**:10009.

Robert Baillie, G. V. Cormack & H. C. Williams, The problem of Sierpiński concerning $k \cdot 2^n+1$, *Math. Comput.*, **37**(1981) 229–231; corrigendum, **39**(1982) 308.

Wieb Bosma, Explicit primality criteria for $h \cdot 2^k \pm 1$, *Math. Comput.*, **61**(1993) 97–109.

D. A. Buell & J. Young, Some large primes and the Sierpiński problem, SRC Technical Report 88-004, Supercomputing Research Center, Lanham MD, May 1988.

G. V. Cormack & H. C. Williams, Some very large primes of the form $k \cdot 2^n+1$, *Math. Comput.*, **35**(1980) 1419–1421; *MR* **81i**:10011; corrigendum, Wilfrid Keller, **38**(1982) 335; *MR* **82k**:10011.

Paul Erdős & Andrew M. Odlyzko, On the density of odd integers of the form $(p-1)2^{-n}$ and related questions, *J. Number Theory*, **11**(1979) 257–263; *MR* **80i**:10077.

G. Jaeschke, On the smallest k such that all $k \cdot 2^N+1$ are composite, *Math. Comput.*, **40**(1983) 381–384; *MR* **84k**:10006; corrigendum, **45**(1985) 637; *MR* **87b**:11009.

Wilfrid Keller, Factors of Fermat numbers and large primes of the form $k \cdot 2^n+1$, *Math. Comput.*, **41**(1983) 661–673; *MR* **85b**:11119; II (incomplete draft, 92-02-19).

Wilfrid Keller, Woher kommen die größten derzeit bekannten Primzahlen? *Mitt. Math. Ges. Hamburg*, **12**(1991) 211–229;*MR* **92j**:11006.

N. S. Mendelsohn, The equation $\phi(x)=k$, *Math. Mag.*, **49**(1976) 37–39; *MR* **53**

#252.
Raphael M. Robinson, A report on primes of the form $k\cdot 2^n+1$ and on factors of Fermat numbers, *Proc. Amer. Math. Soc.*, **9**(1958) 673–681; *MR* **20** #3097.
J. L. Selfridge, Solution of problem 4995, *Amer. Math. Monthly*, **70**(1963) 101.
W. Sierpiński, Sur un problème concernant les nombres $k\cdot 2^n+1$, *Elem. Math.*, **15**(1960) 73–74; *MR* **22** #7983; corrigendum, **17**(1962) 85.
W. Sierpiński, *250 Problems in Elementary Number Theory*, Elsevier, New York, 1970, Problem 118, pp. 10 & 64.
R. G. Stanton & H. C. Williams, Further results on covering of the integers $1+k2^n$ by primes, *Combinatorial Math.* VIII, *Lecture Notes in Math.*, **884**, Springer-Verlag, Berlin–New York, 1980, 107–114.

B22. n！表为 n 个大因子的乘积

Straus, Erdös 和 Selfridge 要求将 n！表示成 n 个因子的乘积,其中最小的因子 l 要尽可能大.例如,对 $n=56, l=15$ 有

$$56! = 15\cdot 16^3\cdot 17^3\cdot 18^8\cdot 19^2\cdot 20^{12}\cdot 21^9\cdot 22^5\cdot 23^2\cdot 26^4 29\cdot 31\cdot 37\cdot 41\cdot 43\cdot 47\cdot 53.$$

Selfridge 有两个猜想:(a)除了 $n=56$ 之外均有 $l\geqslant\lfloor 2n/7\rfloor$;(b)对 $n\geqslant 300000$ 有 $l\geqslant n/3$.如果后者为真,300000 可以减小多少呢?

人们认为 Straus 证明了对 $n>n_0(\varepsilon)$有 $l>n/(e+\varepsilon)$成立这一结论,但在他的遗物中没有找到他的证明.由 Stirling 公式易见这是最好可能的结果.显然,l 是 n 的单调(虽然并非严格单调)增加函数.另一方面,它取不到一切整数值:对 $n=124$ 和 125,l 分别是 35 和 37. Erdös 问 l 的值之间的间隙能有多大? 在任意延伸下去时,l 能否成为常数?

Alladi 和 Grinstead 把 n！表为素数幂的乘积,每个素数幂有 $n^{\delta(n)}$那样大小,又令 $\alpha(n)=\max\delta(n)$,他证明了 $\lim\limits_{n\to\infty}\alpha(n)=e^{c-1}=\alpha$(定义此极限为 α),其中

$$c=\sum_2^{\infty}\frac{1}{k}\ln\frac{k}{k-1},\quad 从而\ \alpha=0.809394020534\cdots.$$

参考文献

K. Alladi & C. Grinstead, On the decomposition of $n!$ into prime powers, *J. Number Theory*, 9(1977) 452–458; *MR* **56** #11934.

P. Erdős, Some problems in number theory, *Computers in Number Theory*, Academic Press, London & New York, 1971, 405–414.

B23. 阶乘分解为若干个阶乘的乘积

设 $n!=a_1!\ a_2!\ \cdots a_r!$, $r\geqslant 2$, $a_1\geqslant a_2\geqslant\cdots\geqslant a_r\geqslant 2$. 一个平凡的例子是 $a_1=a_2!\ \cdots a_r!\ -1$, $n=a_2!\ \cdots a_r!$. Dean Hickerson 注意到,对 $n\leqslant 410$ 仅有的非平凡的例子是 $9!=7!\ 3!\ 3!\ 2!$, $10!=7!\ 6!=7!\ 5!\ 3!$ 以及 $16!=14!\ 5!\ 2!$. 他问是否还有其他的例子了? Jeffrey Shallit 和 Michael Easter 将这一搜索扩大到 $n=18160$.

Erdös 注意到,若 $P(n)$是 n 的最大素因子,且如果已知 $P(n(n+1))/\ln n$ 与 n 一同趋向于无穷,那么便可推出仅有有限多个非平凡的例子.

他和 Graham 研究了方程 $y^2=a_1!\ a_2!\ \cdots a_r!$. 他们定义集合 F_k 由那些 m 组成:对此 m 存在一组整数 $m=a_1>a_2>\cdots>a_r$ $(r\leqslant k)$,它们对某个 y 满足此方程. 又将 F_k-F_{k-1}记为 D_k. 他们得到了各种结果,例如,对几乎所有素数 p, $13p$ 都不属于 F_5, D_6 中最小的数是 527. 若 $D_4(n)$表示 D_4 中$\leqslant n$ 的元素个数,他们不知道 $D_4(n)$增长的阶. 他们猜想 $D_6(n)>cn$ 但不能证明之.

参考文献

Earl Ecklund & Roger Eggleton, Prime factors of consecutive integers, *Amer. Math. Monthly*, **79**(1972) 1082–1089.

E. Ecklund, R. Eggleton, P. Erdős & J. L. Selfridge, on the prime factorization of binomial coefficients, *J. Austral. Math. Soc. Ser. A*, **26**(1978) 257–269; *MR* **80e**:10009.

P. Erdős, Problems and results on number theoretic properties of consecutive integers and related questions, *Congressus Numerantium XVI* (Proc. 5th

Manitoba Conf. Numer. Math. 1975), 25–44.
P. Erdős & R. L. Graham, On products of factorials, *Bull. Inst. Math. Acad. Sinica, Taiwan*, 4(1976) 337–355.

B24. 无一能整除另外两个数的最大集合

令 $f(n)$为$[1,n]$中无一能整除另外两个数的最大子集的大小. Erdös问 $f(n)$能有多大? 取$[m+1,3m+2]$易见 $f(n)$能取到$\lceil 2n/3\rceil$. D.J. Kleitman取$[11,30]$并略去 18,24 和 30,这使我们可以添加 6,8,9 和 10,从而得到 $f(29)=21$. 然而,这个例子似乎无法推广. 实际上 Lebensold证明了,如果 n 很大,那么

$$0.6725n \leqslant f(n) \leqslant 0.6736n.$$

Erdös还问极限 $\lim f(n)/n$ 是否是无理数?

对偶地,人们可以寻求最大数量的$\leqslant n$ 的数,其中无一能是另外任何两个数的倍数. Kleitman的例子也可用作此问题的实例. 更一般地,Erdös希望寻求最大数量的数,使得对 $k>2$ 其中无一能被其他任何 k 个数整除. 对 $k=1$,答案是$\lceil n/2\rceil$.

对一些有关的问题,见 E2.

参 考 文 献

Driss Abouabdillah & Jean M. Turgeon, On a 1937 problem of Paul Erdős concerning certain finite sequences of integers none divisible by another, Proc. 15th S.E. Conf. Combin. Graph Theory Comput., Baton Rouge, 1984, *Congr. Numer.*, **43**(1984) 19–22; *MR* **86h**:11020.
P. Erdős, On a problem in elementary number theory and a combinatorial problem, *Math. Comput.*, (1964) 644–646; *MR* **30** #1087.
Kenneth Lebensold, A divisibility problem, *Studies in Appl. Math.*, **56**(1976–77) 291–294; *MR* **58** #21639.
Emma Lehmer, Solution to Problem 3820, *Amer. Math. Monthly*, **46**(1939) 240–241.

B25. 公比为素数的几何级数之和

Bateman 问:是否 $31=(2^5-1)/(2-1)=(5^3-1)/(5-1)$是

惟一的可以用多于一种方式表成形状如$(p^r-1)/(p-1)$的素数?这里 p 是素数,$r\geqslant 3$ 和 $d\geqslant 1$ 都是整数. 平凡地有 $7=(2^3-1)/(2-1)=((-3)^3-1)/(-3-1)$,但是在$<10^{10}$的范围内不再有其他的数了. 若将 p 是素数这一条件放宽,问题可追溯到 Goormaghtigh,且我们有解

$$8191=(2^{13}-1)/(2-1)=(90^3-1)/(90-1).$$

E. T. Parker 注意到:如果能证明$(p^q-1)/(p-1)$永远不会整除$(q^p-1)/(q-1)$的话(这里 p,q 是不同的奇素数),由 Feit 和 Thompson 对"每个奇数阶群皆为可解群"所作的很长的证明将会被简化. 事实上人们曾猜想,这两个表达式是互素的,但 Nelson Stephens 发现,当 $p=17$, $q=3313$ 时它们有公因子 $2pq+1=112643$. Mckay 证明了,对 $p<53\cdot 10^6$ 有 $p^2+p+1\nmid 3^p-1$.

参考文献

P. T. Bateman & R. M. Stemmler, Waring's problem for algebraic number fields and primes of the form $(p^r-1)/(p^d-1)$, *Illinois J. Math.*, **6**(1962) 142–156; *MR* **25** #2059.

Ted Chinburg & Melvin Henriksen, Sums of kth powers in the ring of polynomials with integer coefficients, *Bull. Amer. Math. Soc.*, **81**(1975) 107–110; *MR* **51** #421; *Acta Arith.*, **29**(1976) 227–250; *MR* **53** #7942.

A. Mąkowski & A. Schinzel, Sur l'équation indéterminée de R. Goormaghtigh, *Mathesis*, **68**(1959) 128–142; *MR* **22** # 9472; **70**(1965) 94–96.

N. M. Stephens, On the Feit-Thompson conjecture, *Math. Comput.*, **25**(1971) 625; *MR* **45** #6738.

B26. 无 l 个两两互素元素的最稠密集

Erdös 问道:使得诸整数 $a_i(1\leqslant a_1<a_2<\cdots<a_k\leqslant n)$中不存在 l 个两两互素的元素的最大的k 是多少? 他猜想这等于$\leqslant n$ 的整数中以头 $l-1$ 个素数中的一个作为其因子的那种数的个数. 他说 $l=2$ 是容易证明的,$l=3$ 的证明也不难. 他对一般的解悬赏 10 美元.

对偶地,我们可以求$[1,n]$的最大子集,该子集中的元素两两有不超过 n 的最小公倍数. 如果用 $g(n)$表示这样一个最大子集

的基数,则 Erdös 证明了

$$\frac{3}{2\sqrt{2}}n^{1/2}-2<g(n)\leqslant 2n^{1/2},$$

其中第一个不等式可如下得到:从 1 到$(n/2)^{1/2}$取整数,同时从$(n/2)^{1/2}$到$(2n)^{1/2}$取偶整数. Choi 将上界改进为 $1.638n^{1/2}$.

参 考 文 献

S. L. G. Choi, The largest subset in [1, n] whose integers have pairwise l.c.m. not exceeding n, *Mathematika*, **19**(1972) 221–230; **47** #8461.

S. L. G. Choi, On sequences containing at most three pairwise coprime integers, *Trans. Amer. Math. Soc.*, **183**(1973) 437–440; **48** #6052.

P. Erdős, Extremal problems in number theory, *Proc. Sympos. Pure Math. Amer. Math. Soc.*, **8**(1965) 181–189; *MR* **30** #4740.

B27. $n+k$ 的不整除 $n+i(0\leqslant i<k)$的素因子个数

Erdös 和 Selfridge 定义 $v(n;k)$为 $n+k$ 的不整除$n+i(0\leqslant i<k)$的素因子个数,定义 $v_0(n)$为当取过所有 $k\geqslant 0$ 时 $v(n;k)$的最大值. 当 n 趋于无穷时有 $v_0(n)\to\infty$吗? 他们证明了,对除了 1,2,3,4,7,8,16 以外的所有 n 有 $v_0(n)>1$. 更一般地,定义 $v_l(n)$为当取过所有 $k\geqslant l$ 时 $v(n;k)$的最大值. 当 n 趋于无穷时有 $v_l(n)\to\infty$吗? 他们甚至不能证明 $v_1(n)=1$ 只有有限多个解. 使 $v_1(n)=1$ 成立的最大的 n 可能是 330.

他们还用 $V(n;k)$来记使得 p^α 是使 p 整除 $n+k$ 但 p^α 不整除$n+i$(对 $0\leqslant i<k$)的最高幂,用 $V_l(n)$记当取过所有 $k\geqslant l$ 时 $V(n;k)$的最大值. 那么 $V_1(n)=1$ 只有有限多个解吗? 可能 $n=80$ 是最大的解. 使 $V_0(n)=2$ 的最大的 n 是什么?

某些进一步的问题写在他们的论文中.

参 考 文 献

P. Erdős & J. L. Selfridge, Some problems on the prime factors of consecutive integers, *Illinois J. Math.*, **11**(1967) 428–430.

A. Schinzel, Unsolved problem 31, *Elem. Math.*, **14**(1959) 82–83.

B28. 有不同素因子的相邻整数

Selfridge 问道：是否存在 n 个相邻整数，每个数或者有两个小于 n 的不同的素因子，或者有一个小于 n 的重素因子？他给出了两个例子：

1. 数 $a+11+i(1\leqslant i\leqslant n=115)$，其中 $a\equiv 0 \bmod 2^2\cdot 3^2\cdot 5^2\cdot 7^2\cdot 11^2$ 且对每个素数 $p(13\leqslant p\leqslant 113)$ 有 $a+p\equiv 0 \bmod p^2$；

2. 数 $a+31+i(1\leqslant i\leqslant n=1329)$，其中对每个素数 $p(37\leqslant p\leqslant 1327)$ 有 $a+p\equiv 0 \bmod p^2$ 及 $a\equiv 0 \bmod 2^2\cdot 3^2\cdot 5^2\cdot 7^2\cdot 11^2\cdot 13^2\cdot 17^2\cdot 19^2\cdot 23^2\cdot 29^2\cdot 31^2$

找寻 n 个相邻整数，其中每个数要么可被两个小于 n 的不同素数整除，要么被一个 $<n/2$ 的素数的平方整除. 这是很困难的，尽管他相信这些数可以用计算机找到.

它与下述问题有关：求 n 个相邻整数，每个数与其他 $n-1$ 个数的乘积有一个合数作为其公因子. 如果合数这一条件予以放宽，仅要求有大于 1 的公因子，那么 $2184+i(1\leqslant i\leqslant n=17)$ 就是一个极好的例子.

参考文献

Alfred Brauer, On a property of k consecutive integers, *Bull. Amer. Math. Soc.*, **47**(1941) 328–331; *MR* **2**, 248.

Ronald J. Evans, On blocks of N consecutive integers, *Amer. Math. Monthly*, **76**(1969) 48–49.

Ronald J. Evans, On N consecutive integers in an arithmetic progression, *Acta Sci. Math. Univ. Szeged*, **33**(1972) 295–296; *MR* **47** #8408.

Heiko Harborth, Eine Eigenschaft aufeinanderfolgender Zahlen, *Arch. Math. (Basel)* **21**(1970) 50–51; *MR* **41** #6771.

Heiko Harborth, Sequenzen ganzer Zahlen, *Zahlentheorie* (*Tagung, Math. Forschungsinst. Oberwolfach*, 1970) 59–66; *MR* **51** #12775.

S. S. Pillai, On m consecutive integers I, *Proc. Indian Acad. Sci. Sect. A*, **11**(1940) 6–12; *MR* **1**, 199; II **11**(1940) 73–80; *MR* **1**, 291; III **13**(1941) 530–533; *MR* **3**, 66; IV *Bull. Calcutta Math. Soc.*, **36**(1944) 99–101; *MR* **6**, 170.

B29. x 是否可以由 $x+1, x+2, \cdots, x+k$ 的素因子所确定?

Allan R. Woods 问道:是否存在正整数 k,使得每个 x 可以由 $x+1, x+2, \cdots, x+k$ 的素因子集合所惟一确定? 可能 $k=3$?

对小于 23 的素数,当 $k=2$ 时有四种不确定的情形:$(x+1, x+2)=(2,3)$或$(8,9)$;$(6,7)$或$(48,49)$;$(14,15)$或$(224,225)$以及$(75,76)$或$(1215,1216)$. 其中的头三个是无穷族$(2^n-2, 2^n-1)$,$(2^n(2^n-2), (2^n-1)^2)$中的元素,比较 B19.

参考文献

D. H. Lehmer, On a problem of Størmer, *Illinois J. Math.*, 8(1964) 57-79; *MR* 28 #2072.

B30. 乘积为平方数的小集合

Erdös,Graham 和 Selfridge 希望我们求 t_n 的最小值,使得整数 $n+1, n+2, \cdots, n+t_n$ 包含一个子集,该子集中的元素和 n 的乘积是一个平方数. Thue-Siegel 定理蕴含当 n 趋于无穷时有 $t_n \to \infty$(其趋于无穷的速度比 $\ln n$ 的幂要快). Selfridge 证明了 $t_n \leqslant \max(P(n), 3\sqrt{n})$,这里 $P(n)$是 n 的最大素因子.

另一方面,是否对每个 c 都存在一个 n_0,使得对每个 $n>n_0$ 乘积 $\prod a_i$ 全不相同? 这里的乘积取过 $n<a_1<\cdots<a_k<n+(\ln n)^c (k=1,2,\cdots)$. 他们对 $c<2$ 证明了此结论.

Selfridge 猜想:如果 n 不是平方数,t 是下一个比 n 大且使 nt 为平方数的数,那么除了 $n=8$ 和 392 以外,总能找到适合 $n<r<s<t$ 的 r 和 s,使 nrs 为平方数. 例如,若 $n=240=2^4\cdot3\cdot5$,那么 $t=375=3\cdot5^3$,我们可求得 $r=243=3^5$ 及 $s=245=5\cdot7^2$.

参考文献

P. Erdős & Jan Turk, Products of integers in short intervals, *Acta Arith.*, **44**(1984) 147–174; *MR* **86d**:11073.

B31. 二项系数

Earl Ecklund，Roger Eggleton，Erdős 和 Selfridge(见 B23)把**二项系数**(binomial coefficient)$\binom{n}{k}=n!/k!(n-k)!$ 写成乘积 UV，这里 U 的每个素因子至多为k，而 V 的每个素因子都大于 k. 对 $n\geqslant 2k$，满足 $U>V$ 的情形仅有有限多种. 除了 $k=3,5,7$ 以外，他们确定了所有这样的情形.

S. P. Khare 列出了 $n\leqslant 551$ 的所有情形：$k=3$，$n=8,9,10,18,82,162$；$k=5$，$n=10,12,28$；以及 $k=7$，$n=21,30,54$.

大多数适合 $n\geqslant 2k$ 的二项系数$\binom{n}{k}$有一个素因子 $p\leqslant n/k$. 在与 Lacampagne 和 Erdős 进行计算之后，Selfridge 猜想：只要 $n>17.125k$，该不等式皆成立. 一个稍强一点的猜想是：除了 4 个例外$\binom{62}{6}$，$\binom{959}{56}$，$\binom{474}{66}$，$\binom{284}{28}$(对它们分别有 $p=19,19,23$ 和 29)，任何这样的二项系数的最小素因子要么 $p\leqslant n/k$，要么 $p\leqslant 17$.

这些作者定义二项系数$\binom{n+k}{k}$($k\leqslant n$)的**亏格**(deficiency)为使 $b_i=1$ 的 i 的个数，其中 $n+i=a_ib_i$($1\leqslant i\leqslant k$)，b_i 的素因子大于k，且 $\prod a_i=k!$，那么

$\binom{44}{8}$，$\binom{74}{10}$，$\binom{174}{12}$，$\binom{239}{14}$，$\binom{5179}{27}$，$\binom{8413}{28}$，$\binom{8414}{28}$和$\binom{96622}{42}$中的每一个都有亏格 2；$\binom{46}{10}$，$\binom{47}{10}$，$\binom{241}{16}$，$\binom{2105}{25}$，$\binom{1119}{27}$和

$\binom{6459}{33}$有亏格 3；$\binom{47}{11}$有亏格 4；而$\binom{284}{28}$有亏格 9. 他们猜想没有其他亏格大于 1 的了. 那么是否只有有限多个二项系数有亏格 1 呢？

Erdös 和 Selfridge 注意到：如果 $n \geqslant 2k \geqslant 4$，则至少有一个 i 的值（$0 \leqslant i \leqslant k-1$）使 $n-i$ 不整除$\binom{n}{k}$. 他们要求最小的 n_k，使得只有一个这样的 i 存在. 例如，$n_2=4$，$n_3=6$，$n_4=9$，$n_5=12$. 又对 $k \geqslant 3$ 有 $n_k \leqslant k!$.

Harry Ruderman 希望给出下述结论的证明或反例：对每对非负整数（p，q），存在一个正整数 n 使

$$\frac{(2n-p)!}{n!(n+q)!}$$

是整数.

一个使优秀数学家也一时困惑不已的问题是：$\binom{n}{r}$与$\binom{n}{s}$互素吗（$0<r<s \leqslant n/2$）？由恒等式

$$\binom{n}{s}\binom{s}{r}=\binom{n}{r}\binom{n-r}{s-r}$$

可对它给出否定的回答. Erdös 和 Szekeres 问：最大公因子的最大素因子是否总大于 r？对 $r>3$ 他们发现的惟一的反例是

$$\gcd\left(\binom{28}{5},\binom{28}{14}\right)=2^3 \cdot 3^3 \cdot 5.$$

Wolstenholme 定理是说：如果 n 是一个 >3 的素数，那么

$$\binom{2n-1}{n} \equiv 1 \bmod n^3.$$

James P. Jones 问其逆是否为真？有关二项系数的因子的其他问题和结果，见 B33.

参考文献

D. F. Bailey, Two p^3 variations of Lucas's theorem, *J. Number Theory*, **35**(1990) 208 215; *MR* **90f**:11008.

Paul Erdős, C. B. Lacampagne & J. L. Selfridge, Estimates of the least prime factor of a binomial coefficient, *Math. Comput.*, **61**(1993) 215–224; *MR* **93k**:11013.
P. Erdős & J. L. Selfridge, Problem 6447, *Amer. Math. Monthly*, **90**(1983) 710; **92**(1985) 435–436.
P. Erdős & G. Szekeres, Some number theoretic problems on binomial coefficients, *Austral. Math. Soc. Gaz.*, **5**(1978) 97–99; *MR* **80e**:10010 is uninformative.
Richard J. McIntosh, A generalization of a congruential property of Lucas, *Amer. Math. Monthly*, **99**(1992) 231–238.
Harry D. Ruderman, Problem 714, *Crux Math.*, **8**(1982) 48; **9**(1983) 58.
David Segal, Problem E435, partial solution by H.W. Brinkman, *Amer. Math. Monthly*, **48**(1941) 269–271.

B32. Grimm 猜想

Grimm 猜想：如果 $n+1, n+2, \cdots, n+k$ 全都是合数，则存在不同的素数 p_{i_j} 使 $p_{i_j} \mid (n+j)$（对 $1 \leqslant j \leqslant k$）. 例如

1802 1803 1804 1805 1806 1807 1808 1809 1810

可分别被

53 601 41 19 43 139 113 67 181

整除，而

114 115 116 117 118 119 120 121 122 123 124 125 126

则分别被

19 23 29 13 59 17 2 11 61 41 31 5 7

整除.

Ramachandra，Shorey 和 Tijdeman 根据 A2 中提到的 Schinzel 的猜想证明了：Grimm 猜想仅有有限多个例外.

Erdös 和 Selfridge 要求 $f(n)$ 的估计式，这里 $f(n)$ 是满足下列条件的最小的数：对每个 m，在区间 $[m+1, m+f(n)]$ 中有使 $p_i \mid a_i$（p_i 是第 i 个素数）成立的不同的整数 $a_1, a_2, \cdots, a_{\pi(n)}$ 存在. 他们和 Pomerance 证明了，对大的 n 有

$$(3-\varepsilon)n \leqslant f(n) \ll n^{3/2}(\ln n)^{-1/2}.$$

参考文献

P. Erdős, Problems and results in combinatorial analysis and combinatorial number theory, in *Proc. 9th S.E. Conf. Combin. Graph Theory, Comput., Boca*

Raton, Congressus Numerantium XXI, Utilitas Math. Winnipeg, 1978, 29-40.
P. Erdös & C. Pomerance, Matching the natural numbers up to n with distinct multiples in another interval, *Nederl. Akad. Wetensch. Proc. Ser. A*, **83**(= *Indag. Math.*, **42**)(1980) 147-161; *MR* **81i**:10053.
Paul Erdös & Carl Pomerance, An analogue of Grimm's problem of finding distinct prime factors of consecutive integers, *Utilitas Math.*, **24**(1983) 45-46; *MR* **85b**:11072.
P. Erdős & J. L. Selfridge, Some problems on the prime factors of consecutive integers II, in *Proc. Washington State Univ. Conf. Number Theory*, Pullman, 1971, 13-21.
C. A. Grimm, A conjecture on consecutive composite numbers, *Amer. Math. Monthly*, **76**(1969) 1126-1128.
Michel Langevin, Plus grand facteur premier d'entiers en progression arithmétique, *Sém. Delange-Pisot-Poitou*, **18**(1976/77) *Théorie des nombres: Fasc.* 1, *Exp. No.* 3, Paris, 1977; *MR* **81a**:10011.
Carl Pomerance, Some number theoretic matching problems, in *Proc. Number Theory Conf.*, Queen's Univ., Kingston, 1979, 237-247.
Carl Pomerance & J. L. Selfridge, Proof of D.J. Newman's coprime mapping conjecture, *Mathematika*, **27**(1980) 69-83; *MR* **81i**:10008.
K. Ramachandra, T. N. Shorey & R. Tijdeman, On Grimm's problem relating to factorization of a block of consecutive integers, *J. reine angew. Math.*, **273**(1975) 109-124.

B33. 二项系数的最大因子

有关二项系数 $\binom{n}{k}=n!/k!(n-k)!$ 的小于 n 的最大因子,我们能说些什么呢? Erdös 指出,容易证明它至少是 n/k,并猜想:对任何 $c<1$ 及充分大的 n,它可能在 cn 和 n 之间. Marilyn Faulkner 证明了:如果 p 是 $>2k$ 的最小素数且 $n\geqslant p$,那么除了 $\binom{9}{2}$ 和 $\binom{10}{3}$ 以外,$\binom{n}{k}$ 都有一个 $\geqslant p$ 的素因子. Earl Ecklund 证明了:如果 $n\geqslant 2k>2$,那么除了 $\binom{7}{3}$ 以外,$\binom{n}{k}$ 都有一个素因子 $p\leqslant n/2$.

John Selfridge 猜想:如果 $n\geqslant k^2-1$,那么除了例外值 $\binom{62}{6}$ 以

外，$\binom{n}{k}$都有一个素因子 $p\leqslant n/k$. 在最小素因子 $p\geqslant n/k$ 的那些二项系数中，可能只有有限多个满足 $p\geqslant 13$，但可能有无穷多个二项系数使其最小素因子 $p=7$. 而存在无穷多个使 $p=5$ 这一结论已由 Erdös, Lacampagne 和 Selfridge 予以证明(B31).

由 Sylvester 和 Schur 相互独立地发现的一个经典定理是说：k 个均大于 k 的相邻整数的乘积必有一个大于 k 的素因子. Leo Moser 猜想 Sylvester-Schur 定理对 $\equiv 1 \bmod 4$ 的素数成立，其含义如下：对充分大的 $n(\geqslant 2k)$，$\binom{n}{k}$有一个大于 k 的素因子 $\equiv 1 \bmod 4$. 然而，Erdös 并不认为此猜想为真，但它可能并不容易解决. 对此，John Leech 注意到：14 个整数 280213，…，280226 并没有形如 $4m+1>13$ 的素因子.

由于 Ira Gessel 和 John Conway 的贡献我们才能说：在本书第一版中由 Neil Sloane 提出的 **Catalan 数**(Catalan number) $\frac{1}{n+1}\binom{2n}{n}$的推广(即$\frac{(n,r)}{n}\binom{n}{r}$)总是一个整数(乘以 n 和 r，而 Euclid 知道 (n,r) 是 n 和 r 的线性组合). 这些数也称为推广的抽签数(ballot number)，当对某种格路径(lattice path)进行计数时就会出现这种数.

若用 $f(n)$ 表示 $<n$ 且不整除$\binom{2n}{n}$的素数的倒数之和，则 Erdös, Graham, Ruzsa 和 Straus 猜想：存在绝对常数 c，使对所有 n 有 $f(n)<c$. Erdös 还猜想：对 $n>4$，$\binom{2n}{n}$从不为无平方因子数. 由于 $4\left|\binom{2n}{n}\right.$(除非 $n=2^k$)，故只需考虑

$$\binom{2^{k+1}}{2^k}$$

即可. Sárközy 对充分大的 n 证明了这一猜想，而 Sander 则证明

了：在一种精确的意义下，接近 Pascal 三角中心处的二项系数不是无平方因子数. Granville 和 Rammaré 对大到 $k>300000$ 的值用证明，而对 $2\le k\le300000$ 内的值用计算完成了 Sárközy 的证明. 他们还改进了 Sander 的结果，即证明了存在常数 $\delta, 0<\delta<1$，使得只要 $\binom{n}{k}$ 无平方因子，对充分大的 n 必有 k 或 $n-k<n^{\delta}$. 他们猜想事实上必有 k 或 $n-k<(\ln n)^{2-\delta}$，且在下述意义上来说这是最好可能的结果：对某个 $c>0$ 存在无穷多个 $\binom{n}{k}$ 适合 $\frac{1}{2}n>k>c(\ln n)^2$. 他们对 $\frac{1}{2}n>k>\frac{1}{5}\ln n$ 证明了此结果. 他们指出：存在一个常数 $\rho_k>0$，在 $n\leqslant N$ 中使 $\binom{n}{k}$ 无平方因子的数的个数 $\sim\rho_k N$. 由于对某个 $c>0$ 有 $\rho_k<c/k^2$，故而他们猜想：存在一个常数 $\gamma>0$，使 Pascal 三角的前 N 行中无平方因子数的个数是 $\sim\gamma N$.

Erdös 又猜想：对 $k>8$，2^k 不是 3 的不同的幂之和 $[2^8=3^5+3^2+3+1]$. 若果然如此，则对 $k\geqslant9$ 有

$$3\left|\binom{2^{k+1}}{2^k}\right..$$

为了回答"$\binom{342}{171}$ 是否是不被奇素数的平方整除的最大的 $\binom{2n}{n}$"这一问题，Eugene Levine 给出例子 $n=784$ 和 786. Erdös 确信不再有这样更大的 n 了.

用 $e=e(n)$ 记对某个素数 p 使 p^e 为整除 $\binom{2n}{n}$ 的最大幂. 还不知道是否有 $e\to\infty(n\to\infty$ 时)? 另一方面 Erdös 无法推翻结论 $e>c\ln n$.

Ron Graham 悬赏 100 美元以确定是否无穷常有 $\left(\binom{2n}{n},105\right)=1$. Kummer 知道，当用基 3,5 或 7 来表达时，n 只能分别有数字 0,1;0,1,2 或 0,1,2,3. H. Gupta 和 S. P. Khare 发

现了小于 7^{10}的 14 个 n 的值：1，10，756，757，3160，3186，3187，3250，7560，7561，7651，20007，59548377，59548401．而 Peter Montgomery，Khare 和其他人找到了许多更大的值．

Erdös，Graham，Ruzsa 和 Straus 证明了：对任何两个素数 p 和 q，存在无穷多个 n 使

$$\left(\binom{2n}{n}, pq\right) = 1.$$

如果 $g(n)$是$\binom{2n}{n}$的最小奇素因子，则 $g(3160)=13$，且对 $3160<n<10^{10000}$有 $g(n)\leqslant 11$．

参考文献

E. F. Ecklund, On prime divisors of the binomial coefficient, *Pacific J. Math.*, **29**(1969) 267–270.

P. Erdős, A theorem of Sylvester and Schur, *J. London Math. Soc.*, **9**(1934) 282–288.

Paul Erdős, A mélange of simply posed conjectures with frustratingly elusive solutions, *Math. Mag.*, **52**(1979) 67–70.

P. Erdős & R. L. Graham, On the prime factors of $\binom{n}{k}$, *Fibonacci Quart.*, **14**(1976) 348–352.

P. Erdős, R. L. Graham, I. Z. Ruzsa & E. Straus, On the prime factors of $\binom{2n}{n}$, *Math. Comput.*, **29**(1975) 83–92.

M. Faulkner, On a theorem of Sylvester and Schur, *J. London Math. Soc.*, **41**(1966) 107–110.

Andrew Granville & Olivier Ramaré, Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients (see Abstract 882-11-124, *Abstracts Amer. Math. Soc.*, **14**(1993) 419.)

Hansraj Gupta, On the parity of $(n+m-1)!(n,m)/n!m!$, *Res. Bull. Panjab Univ.* (*N.S.*), **20**(1969) 571–575; *MR* **43** #3201.

L. Moser, Insolvability of $\binom{2n}{n}=\binom{2a}{a}\binom{2b}{b}$, *Canad. Math. Bull.*, **6**(1963)167–169.

J. W. Sander, Prime power divisors of $\binom{2n}{n}$, *J. Number Theory*, **39**(1991) 65–74; *MR* **92i**:11097.

J. W. Sander, On prime divisors of binomial coefficients, *Bull. London Math. Soc.*, **24**(1992) 140–142; *MR* **93g**:11019.

J. W. Sander, Prime power divisors of binomial coefficients, *J. reine angew. Math.*, **430**(1992) 1–20; *MR* **93h**:11021; reprise **437**(1993) 217–220.

J. W. Sander, On primes not dividing binomial coefficients, *Math. Proc. Cambridge Philos. Soc.*, **113**(1993) 225–232; *MR* **93m**:11099.

J. W. Sander, An asymptotic formula for ath powers dividing binomial coeffi-

cients, *Mathematika*, **39**(1992) 25–36; *MR* **93i**:11110.
J. W. Sander, On primes not dividing binomial coefficients, *Math. Proc. Cambridge Philos. Soc.*, **113**(1993) 225–232.
A. Sárközy, On divisors of binomial coefficients I, *J. Number Theory*, **20**(1985) 70–80; *MR* **86c**:11002.
Renate Scheidler & Hugh C. Williams, A method of tabulating the number-theoretic function $g(k)$, *Math. Comput.*, **59**(1992) 251–257; *MR* **92k**:11146.
I. Schur, Einige Sätze über Primzahlen mit Anwendungen und Irreduzibilitätsfragen I, *S.-B. Preuss, Akad. Wiss. Phys.-Math. Kl.*, **14**(1929) 125–136.
J. Sylvester, On arithmetical series, *Messenger of Math.*, **21**(1892) 1–19, 87–120.
W. Utz, A conjecture of Erdős concerning consecutive integers, *Amer. Math. Monthly*, **68**(1961) 896–897.

B34. 是否存在 i 使 $n-i$ 整除 $\binom{n}{k}$?

若 $H_{k,n}$ 是如下命题：存在一个 i, $0\leqslant i<k$, 使 $n-i$ 整除 $\binom{n}{k}$. 那么 Erdös 问：当 $n\geqslant 2k$ 时，$H_{k,n}$ 是否对所有的 k 为真? Schinzel 给出一个反例：$n=99215$, $k=15$. 若 H_k 是如下命题：$H_{k,n}$ 对所有的 n 为真，那么 Schinzel 证明了 H_k 对 $k=15,21,22,33,35$ 和 k 的其他 13 个值不真. 他证明了：对所有其余的 $k\leqslant 32$, H_k 为真. 他又问是否有无穷多个非素数幂的 k 使 H_k 为真. 他猜想此结论不真. 后来他又报告说此结论对 $k=34$ 为真，但对 34 和 201 之间其余的非素数幂不真.

参考文献

E. Burbacka & J. Piekarczyk, P. 217, R. 1, *Colloq. Math.*, **10**(1963) 365.
A. Schinzel, Sur un problème de P. Erdős, *Colloq. Math.*, **5**(1957–58) 198–204.

B35. 有相同素因子的相邻整数的乘积

设 $f(n)$ 为使得数 $n, n+1, \cdots, n+f(n)$ 中至少有一个能整除其余诸数之积的最小整数. 易见 $f(k!)=k$ 且对 $n>k!$ 有 $f(n)>k$. Erdös 还证明了：对无穷多个 n 的值有

$$f(n) > \exp((\ln n)^{1/2-\epsilon}),$$

但看来很难求得 $f(n)$ 的好的上界.

Erdös 问:$(m+1)(m+2)\cdots(m+k)$ 和 $(n+1)(n+2)\cdots(n+l)$(其中 $k\geq l\geq 3$)是否能无穷常有同样的素因子? 例如 $(2\cdot3\cdot4\cdot5\cdot6)\cdot7\cdot8\cdot9\cdot10$ 和 $14\cdot15\cdot16$ 及 $48\cdot49\cdot50$. 又如 $(2\cdot3\cdot4\cdot5\cdot6)\cdot7\cdot8\cdot9\cdot10\cdot11\cdot12$ 和 $98\cdot99\cdot100$. 对 $k=l\geq 3$ 他猜想这仅可能发生有限多次.

若 $L(n;k)$ 是诸数 $n+1, n+2, \cdots, n+k$ 之最小公倍数, 则 Erdös 猜想:对 $l>1$ 和 $n\geq m+k$, $L(m;k)=L(n;l)$ 只有有限多个解. 例如 $L(4;3)=L(13;2)$ 和 $L(3;4)=L(19;2)$. 他问:是否有无穷多个 n, 使对所有 $k(1\leq k<n)$ 有 $L(n;k)>L(n-k;k)$? 使此不等式能反向成立的最大的 $k=k(n)$ 是什么? 他注意到易有 $k(n)=o(n)$, 但他相信还有更进一步的结论成立. 他期望对每个 $\epsilon>0$ 及 $n>n_0(\epsilon)$ 有 $k(n)<n^{1/2+\epsilon}$ 成立, 但却不能证明它.

参考文献

P. Erdős, How many pairs of products of consecutive integers have the same prime factors? *Amer. Math. Monthly*, **87**(1980) 391–392.

B36. Eulerφ 函数

Eulerφ 函数(Euler totient function) $\varphi(n)$ 表示不大于 n 且与 n 互素的整数个数. 例如 $\varphi(1)=\varphi(2)=1$, $\varphi(3)=\varphi(4)=\varphi(6)=2$, $\varphi(5)=\varphi(8)=\varphi(10)=\varphi(12)=4$, $\varphi(7)=\varphi(9)=6$. 是否有无穷多对相邻整数 n 和 $n+1$ 使 $\varphi(n)=\varphi(n+1)$? 例如 $n=1,3,15,104,164,194,255,495,584,975$. 我们甚至不知道对每个 $\epsilon>0$, $|\varphi(n+1)-\varphi(n)|<n^{\epsilon}$ 是否有无穷多个解? Baillie 将其他人的工作加以推广, 在 10^8 以下找到了 $\varphi(n)=\varphi(n+1)$ 的 306 个解, 在 10^8 与 $2\cdot10^8$ 之间找到该方程的 85 个解.

Schinzel 猜想对每个偶数 k，方程 $\varphi(n+k)=\varphi(n)$ 有无穷多个解. 他注意到，对奇的 k 对应的猜想似不成立. 对 $k=1$ 即为上一段所述之问题. 对 $k=3$，他发现在 $n<10^4$ 中只有解 $n=3$ 和 $n=5$. D. H. Lehmer 将此扩大到 10^6. Sierpiński 证明了对每个 k，$\varphi(n+k)=\varphi(n)$ 至少有一个解，而 Schinzel 和 Wakulicz 则证明了对每个 $k<2\cdot10^{58}$ 它至少有两个解. Mąkowski 证明了对每个 k，$\varphi(n+k)=2\varphi(n)$ 至少有一个解. 有关方程 $\varphi(n+k)=3\varphi(n)$ 请看 *Amer. Math. Monthly*, 96(1989) 63－64 中问题 E 3215 的解.

Mąkowski(见问题 B5 的文献)还讨论了方程 $\varphi(x+k)=\varphi(x)+\varphi(k)$. J. Browkin 证明了：如果 $k=3$，则它没有解 $x<37182142$.

三个难得一见的结果是

$$\varphi(5186)=\varphi(5187)=\varphi(5188)=2^5 3^4$$

$$\varphi(25930)=\varphi(25935)=\varphi(25940)=\varphi(25942)=2^7 3^4$$

$$\varphi(404471)=\varphi(404473)=\varphi(404477)=2^8 3^2 5^2 7.$$

非 φ 值(nontotient)指的是使 $\varphi(x)=n$ 无解的正偶数 n，例如 $n=14,26,34,38,50,62,68,74,76,86,90,94,98$. Lehmers 对小于 y 的这种数的个数 $\#(y)$ 进行了计算.

y	10^3	10^4	$2\cdot10^4$	$3\cdot10^4$	$4\cdot10^4$	$5\cdot10^4$	$6\cdot10^4$	$7\cdot10^4$	$8\cdot10^4$	$9\cdot10^4$
$\#(y)$	210	2627	5515	8458	11438	14439	17486	20536	23606	26663

Erdös 和 Hall 证明了：使 $\varphi(x)=n$ 有解的 n 的个数 $\Phi(y)=y-\#(y)$ 是 $ye^{f(y)}/\ln y$，其中 $f(y)$ 在 $c(\ln\ln\ln y)^2$ 与 $c(\ln y)^{1/2}$ 之间. Maier 和 Pomerance 新近证明了上述下界对 $c\approx0.8178$ 为真. Erdös 猜想 $\Phi(cy)/\Phi(y)\to c$. 如此猜想为真，在寻求 $\Phi(y)$ 的渐近公式时这或许是最好的替代物.

非对偶 φ 值(noncototient)是指使 $x-\varphi(x)=n$ 无解的整数 n，例如 $n=10,26,34,50,52,58,86,100$. Sierpiński 和 Erdös 猜想有无穷多个非对偶 φ 值.

Erdös 曾问道下述结论是否为真：对每个 ε 存在一个 n 使 $\varphi(n)=m$，$m<\varepsilon n$，而对 $t<n$，$\varphi(t)=m$ 都不成立. 这样的 n 好

像有许多.

Michael Ecker 问:对 x 的什么样的值,级数

$$\sum_{n=1}^{\infty}\varphi(n)/n^x \text{ 和 } \sum_{n=1}^{\infty}(-1)^{n+1}\varphi(n)/n^x$$

均收敛?

参考文献

Robert Baillie, Table of $\phi(n)=\phi(n+1)$, *Math. Comput.*, **30**(1976) 189–190.

David Ballew, Janell Case & Robert N. Higgins, Table of $\phi(n)=\phi(n+1)$, *Math. Comput.*, **29**(1975) 329–330.

Michael W. Ecker, Problem E-1, *The AMATYC Review*, **5**(1983) 55; comment **6**(1984)55.

P. Erdős, Über die Zahlen der Form $\sigma(n)-n$ und $n-\phi(n)$, *Elem. Math.*, **28**(1973) 83–86.

P. Erdős & R. R. Hall, Distinct values of Euler's ϕ-function, *Mathematika*, **23**(1976) 1–3.

Patricia Jones, On the equation $\phi(x)+\phi(k)=\phi(x+k)$, *Fibonacci Quart.*, **28**(1990) 162–165; *MR* **91e**:11008.

M. Lal & P. Gillard, On the equation $\phi(n)=\phi(n+k)$, *Math. Comput.*, **26**(1972) 579–582.

Helmut Maier & Carl Pomerance, On the number of distinct values of Euler's ϕ-function, *Acta Arith.*, **49**(1988) 263–275.

Andrzej Mąkowski, On the equation $\phi(n+k)=2\phi(n)$, *Elem. Math.*, **29**(1974) 13.

Kathryn Miller, UMT **25**, *Math. Comput.*, **27**(1973) 447-448.

A. Schinzel, Sur l'équation $\phi(x+k)=\phi(x)$, *Acta Arith.*, **4**(1958) 181–184; *MR* **21** #5597.

A. Schinzel & A. Wakulicz, Sur l'équation $\phi(x+k)=\phi(x)$ II, *Acta Arith.*, **5**(1959) 425–426; *MR* **23** #A831.

W. Sierpiński, Sur un propriété de la fonction $\phi(n)$, *Publ. Math. Debrecen*, **4**(1956) 184–185.

Charles R. Wall, Density bounds for Euler's function, *Math. Comput.*, **26** (1972) 779-783 with microfiche supplement; *MR* **48** #6043.

Masataka Yorinaga, Numerical investigation of some equations involving Euler's ϕ-function, *Math. J. Okayama Univ.*, **20**(1978) 51–58.

B37. $\varphi(n)$能否成为 $n-1$ 的真因子?

D. H. Lehmer 猜想不存在合数 n 使 $\varphi(n)$ 为 $n-1$ 的因子,即不存在 n 使 $\varphi(n)$ 为 $n-1$ 的真因子. 这样的 n 必为一个

Carmichael 数(A13). 他证明了这种数必至少是 7 个不同素数的乘积. 而 Lieuwens 证明了,如果$3|n$,则有 $n>5.5\cdot10^{571}$且 $\omega(n)\geqslant 212$;如果 n 的最小素因子是 5,则有 $n\geqslant 11$;如果 n 的最小素因子至少是 7,则有 $\omega(n)\geqslant 13$. 这取代并纠正了 Schuh 的工作. Masao Kishore 证明了在任何情形这种数都至少要有 13 个素因子,Cohn 和 Hagis 将此改进为 14. Siva Rama Prasad 和 Subbarao 将 Lieuwens 的结果 212 改进为 $\omega(n)\geqslant 1850$, 而 Hagis 则又得到 $\omega(n)\geqslant 298848$. Siva Rama Prasad 和 Rangamma 证明了,如果 $3|n$, n 是合数, $M\varphi(n)=n-1$, $M\neq 4$, 那么有 $\omega(n)\geqslant 5334$.

Pomerance 证明了,小于 x 且使 $\varphi(n)|n-1$ 的合数 n 的个数为

$$O(x^{1/2}(\ln x)^{3/4}(\ln\ln x)^{-1/2}),$$

而单墫(Shan Zun)将幂$\frac{3}{4}$改进为$\frac{1}{2}$.

Schinzel 注意到, 如果 $n=p$ 或 $2p$, 这里 p 是素数, 那么 $\varphi(n)+1$整除 n,他还问其逆是否恒为真? Segal(见他与 Cohen 的论文)注意到,Schinzel 的问题可化为 Lehmer 的问题,该问题出现在群论中,可能是由 G. Hajós 提出的(见 Miech 的论文,尽管在该文中它被归属于 Gordon).

如果 n 是素数,那么它整除 $\varphi(n)d(n)+2$. 它对除 $n=4$ 以外的任何合数 n 是否为真? Subbarao 也注意到,如果 n 是素数,那么 $n\sigma(n)\equiv 2\bmod\varphi(n)$;又如果 $n=4,6$ 或 22,此式亦成立. 它是否对无穷多个合数 n 为真?

Subbarao 有一个与 Lehmer 类似的猜想,该猜想基于函数 $\varphi^*(n)=\prod(p^a-1)$, 此乘积取过 n 的最大素数幂因子, $p^a\|n$. 他猜想 $\varphi^*(n)|(n-1)$当且仅当 n 是一个素数幂. 他还有一个与 Lehmer 猜想"对偶的"猜想,即仅当 n 是素数时有 $\psi(n)\equiv 1\bmod n$, 这里 $\psi(n)$是 Dedekind 函数(见 B41).

Ron Graham 给出如下猜想

¿ 对所有 k 有无穷多个 n 使 $\varphi(n)|(n-k)$?

他注意到对 $k=0, k=2^a(a\geq0)$ 及 $k=2^a3^b(a,b>0)$ 此猜想为真. 例如, Pomerance(见问题 B2 中提到的 *Acta Arith*. 上的论文)对 Graham 的问题作了处理. Victor Meally 发现 $\varphi(n)$ 有时整除 $n+1$, 例如对 $n=n_1=3\cdot5\cdot17\cdot353\cdot929$ 和 $n=n_1\cdot83623937$(注意 $353=11\cdot2^5+1, 929=29\cdot2^5+1, 83623937=11\cdot29\cdot2^{18}+1$ 以及 $(353-2^8)(929-2^8)=2^{16}-2^8+1$.).

参考文献

Ronald Alter, Can $\phi(n)$ properly divide $n-1$? *Amer. Math. Monthly*, **80** (1973) 192–193.

G. L. Cohen & P. Hagis, On the number of prime factors of n if $\phi(n)|n-1$, *Nieuw Arch. Wisk.* (3), **28**(1980) 177–185.

G. L. Cohen & S. L. Segal, A note concerning those n for which $\phi(n)+1$ divides n, *Fibonacci Quart.*, **27**(1989)285–286.

Masao Kishore, On the equation $k\phi(M)=M-1$, *Nieuw Arch. Wisk.* (3), **25**(1977) 48–53; see also *Notices Amer. Math. Soc.*, **22**(1975) A501–502.

D. H. Lehmer, On Euler's totient function, *Bull. Amer. Math. Soc.*, **38**(1932) 745–751.

E. Lieuwens, Do there exist composite numbers for which $k\phi(M)=M-1$ holds? *Nieuw Arch. Wisk.* (3), **18**(1970) 165–169; *MR* **42** #1750.

R. J. Miech, An asymptotic property of the Euler function, *Pacific J. Math.*, **19**(1966) 95–107; *MR* **34** #2541.

Carl Pomerance, On composite n for which $\phi(n)|n-1$, *Acta Arith.*, **28**(1976) 387–389; II, *Pacific J. Math.*, **69**(1977) 177–186; *MR* **55** #7901; see also *Notices Amer. Math. Soc.*, **22**(1975) A542.

József Sándor, On the arithmetical functions $\sigma_k(n)$ and $\phi_k(n)$, *Math. Student*, **58**(1990) 49–54; *MR* **91h**:11005.

Fred. Schuh, Can $n-1$ be divisible by $\phi(n)$ when n is composite? *Mathematica*, Zutphen B, **12**(1944) 102–107.

V. Siva Rama Prasad & M. Rangamma, On composite n satisfying a problem of Lehmer, *Indian J. Pure Appl. Math.*, **16**(1985) 1244–1248; *MR* **87g**:11017.

V. Siva Rama Prasad & M. Rangamma, On composite n for which $\phi(n)|n-1$, *Nieuw Arch. Wisk.* (4), **5**(1987) 77–81; *MR* **88k**:11008.

M. V. Subbarao, On two congruences for primality, *Pacific J. Math.*, **52**(1974) 261–268; *MR* **50** #2049.

M. V. Subbarao, On composite n satisfying $\psi(n)\equiv1 \bmod n$, Abstract 882-11-60 *Abstracts Amer. Math. Soc.*, **14**(1993) 418.

David W. Wall, Conditions for $\phi(N)$ to properly divide $N-1$, *A Collection of Manuscripts Related to the Fibonacci Sequence*, 18th Anniv. Vol., Fibonacci Assoc., 205–208.

Shan Zun, On composite n for which $\phi(n)|n-1$, *J. China Univ. Sci. Tech.*, **15**(1985) 109–112; *MR* **87h**:11007.

B38. $\varphi(m)=\sigma(n)$的解

是否有无穷多对数 m,n 使 $\varphi(m)=\sigma(n)$? 因为对素数 p 有 $\varphi(p)=p-1$ 和 $\sigma(p)=p+1$,故只要存在无穷多对孪生素数(A7),此问题的解答就是肯定的.同样地,由于 $\sigma(M_p)=2^p=\varphi(2^{p+1})$,故当存在无穷多个 Mersenne 素数时(A3),此问题也有肯定的解答.然而,除了这些可能的解以外它还有许多解,这些解有时看不出有什么明显的特征,例如 $\varphi(780)=192=\sigma(105)$.

Erdös 注意到方程 $\varphi(x)=n!$ 是可解的,且(除了 $n=2$ 以外)$\sigma(y)=n!$ 可能也是可解的.Charles R. Wall 能证明对 $n\neq2$ 方程 $\psi(n)=n!$ 是可解的,其中 ψ 是 Dedekind 函数(见 B41).

参考文献

Le Mao-Hua, A note on primes p with $\sigma(p^m)=z^n$, *Colloq. Math.*, **62**(1991) 193-196.

B39. Carmichael 猜想

Carmichael 猜想(Carmichael conjeceture). 对每个 n 似乎能找到一个不等于 n 的 m 使有 $\varphi(m)=\varphi(n)$. 在 20 世纪早期的若干年里人们曾以为 Carmichael 已经证明了这一猜想. Klee 对满足 $\varphi(n)<10^{400}$的 n 以及对所有不被 $2^{42}\cdot3^{47}$整除的 n 验证了这一猜想.Massai 和 Valette 将此界提高到 10^{10000},Schlafly 和 Wagon 则改进为 $10^{13600000}$,其后又提高到 $10^{10000000}$. Pomerance 证明了,如果 n 是有如下性质的数:对每个使得 $p-1$ 整除 $\varphi(n)$的素数 p 都有 p^2 整除 n,那么 n 就是一个反例.他还能证明(未发表),如果前 k 个素数 $p\equiv1(\bmod q)$(其中 q 是素数)全都小于 q^{k+1},那么不存在满足此定理的数 n.这也蕴含了他的猜想 $p_k-1\left|\prod\limits_{i<k}p_i(p_i-1)\right.$ 的正确性.最后这一猜想的正确性也蕴含了不存在满足此定理的数

n.

定义一个整数的重数(multiplicity)为它作为 $\varphi(n)$的值出现的次数. 例如,6 的重数是 4,因为对 $n=7,9,14,18$ 有 $\varphi(n)=6$,而对其他的 n 此式皆不成立. 重数可以是零(对任何奇数 $n>1$ 及对 $n=14,26,34,\cdots$),但根据 Carmichael 猜想,重数不能是 1. Sierpiński 猜想所有大于 1 的整数都作为某个数的重数出现;而 Erdös 证明了:如果一个重数出现了一次,它必出现无穷多次. Schlafly 和 Wagon 找到了从 2 到 65 的所有重数的例子.

有这样的偶数 n 存在,对于它不存在奇数 m 使有 $\varphi(m)=\varphi(n)$. Lorraine Foster 作为这样的数中之最小者给出 $n=33817088=2^9\cdot 257^2$.

Erdös 证明了,如果 $\varphi(x)=k$ 恰有 s 个解,则必有另外无穷多个 k 使该方程也恰有 s 个解,且对无穷多个 k 有 $s>k^c$. 如果 C 是使之为真的那种 c 的最小上界,则 Wooldridge 证明了 $C\geqslant 3-2\sqrt{2}>0.17157$. Pomerance 利用 Hooley 对 Brun-Titchmarsh 定理的改进将此结果改进为 $C\geqslant 1-625/512e>0.55092$,他还发现由 Iwaniec作出的进一步的改进使他可以得到 $C>0.55655$,从而对无穷多个 k 有 $s>k^{5/9}$. Erdös 猜想有 $C=1$. 在另外的方向上 Pomerance 证明了

$$s<k\exp\{-(1+o(1))\ln k\ln\ln\ln k/\ln\ln k\},$$

他还给出一种探索式的讨论以支持他认为这是最好可能结果的信念.

参考文献

R. D. Carmichael, Note on Euler's ϕ-function, *Bull. Amer. Math. Soc.*, **28** (1922) 109–110; and see **13**(1907) 241–243.

P. Erdős, On the normal number of prime factors of $p-1$ and some other related problems concerning Euler's ϕ-function, *Quart. J. Math. Oxford Ser.*, **6**(1935) 205–213.

P. Erdős, Some remarks on Euler's ϕ-function and some related problems, *Bull. Amer. Math. Soc.*, **51**(1945) 540–544.

P. Erdős, Some remarks on Euler's ϕ-function, *Acta Arith.*, **4**(1958) 10–19; *MR*

22#1539.
Lorraine L. Foster, Solution to problem E3361, *Amer. Math. Monthly*, **98** (1991) 443.
Peter Hagis, On Carmichael's conjecture concerning the Euler phi function (Italian summary), *Boll. Un. Mat. Ital.* (6), **A5**(1986) 409-412.
C. Hooley, On the greatest prime factor of $p+a$, *Mathematika*, **20**(1973) 135-143.
Henryk Iwaniec, On the Brun-Titchmarsh theorem and related questions, *Proc. Queen's Number Theory Conf., Kingston, Ont. 1979*, Queen's Papers Pure Appl. Math., **54**(1980) 67-78; *Zbl.* **446**.10036.
V. L. Klee, On a conjecture of Carmichael, *Bull. Amer. Math. Soc.*, **53**(1947) 1183-1186; *MR* **9**, 269.
P. Masai & A. Valette, A lower bound for a counterexample to Carmichael's conjecture, *Boll. Un. Mat. Ital. A* (6), **1** (1982) 313-316; *MR* **84b**:10008.
Carl Pomerance, On Carmichael's conjecture, *Proc. Amer. Math. Soc.*, **43** (1974) 297-298.
Carl Pomerance, Popular values of Euler's function, *Mathematika*, **27** (1980) 84-89; *MR* **81k**:10076.
Aaron Schlafly & Stan Wagon, Carmichael's conjecture is valid below $10^{2,000,000}$, *Math. Comput.*
M. V. Subbarao & L.-W. Yip, Carmichael's conjecture and some analogues, in *Théorie des Nombres* (Québec, 1987), de Gruyter, Berlin-New York, 1989, 928-941 (and see *Canad. Math. Bull.*, **34**(1991) 401-404.
Alain Valette, Fonction d'Euler et conjecture de Carmichael, *Math. et Pédag.*, Bruxelles, **32**(1981) 13-18.
Stan Wagon, Carmichael's 'Empirical Theorem', *Math. Intelligencer*, **8**(1986) 61-63; *MR* **87d**:11012.
K. R. Wooldridge, Values taken many times by Euler's phi-function, *Proc. Amer. Math. Soc.*, **76**(1979) 229-234; *MR* **80g**:10008.

B40. 小于 n 且与 n 互素的数相互之间的间隙

如果 $a_1 < a_2 < \cdots < a_{\varphi(n)}$ 是小于 n 且与之互素的整数,则 Erdös 猜想有 $\sum (a_{i+1} - a_i)^2 \ll cn^2/\varphi(n)$,并为此证明悬赏 500 美元. Hooley 证明了:对 $1 \leqslant \alpha < 2$ 有 $\sum (a_{i+1} - a_i)^\alpha \ll n(n/\varphi(n))^{\alpha-1}$ 以及 $\sum (a_{i+1} - a_i)^2 \ll n(\ln\ln n)^2$;Vaughan"在平均的意义上"证实了这一猜想,并最终与 Montgomery 一道赢得了这笔奖金.

Jacobsthal 问:$J(n) = \max(a_{i+1} - a_i)$ 的界是什么? Erdös 问:对无穷多个 x,是否有两个整数 n_1, n_2 ($n_1 < n_2 < x$, $n_1 \perp n_2$,)存

在，使 $J(n_1)>\ln x$，$J(n_2)>\ln x$？

参考文献

P. Erdős, On the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal, *Math. Scand.*, **10**(1962) 163–170; *MR* **26** #3651.

C. Hooley, On the difference of consecutive numbers prime to n, *Acta Arith.*, **8**(1962/63) 343–347; *MR* **27** #5741.

H. L. Montgomery & R. C. Vaughan, On the distribution of reduced residues, *Ann. of Math.* (2), **123**(1986) 311–333; *MR* **87g**:11119.

R. C. Vaughan, Some applications of Montgomery's sieve, *J. Number Theory*, **5**(1973) 64–79.

B41. φ 和 σ 的迭代

因子之和与单因子之和这两个函数之间有一个密切的联系，单因子函数是对 Euler 函数的一种补充，它常以 Dedekind 函数命名。如果 $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$，用 $\psi(n)$ 表示乘积 $\prod p_i^{a_i-1}(p_i+1)$，也即 $\psi(n)=n\prod(1+p^{-1})$，这里乘积取过 n 的不同素因子。易见 ψ 函数的迭代最终变为形如 2^a3^b 的项，其中 b 固定而 a 连续增加。给定任一 b 的值，都有无穷多个 n 的值导致这样的项，例如 $\psi^k(2^a3^b7^c)=2^{a+4k}3^b7^{c-k}$ $(0\le k\le c)$ 和 $\psi^k(2^a3^b7^c)=2^{a+5k-c}3^b$ $(k>c)$。

David E. Penney 和 Pomerance 在一篇未发表的论文里证明了：存在 n 的值，使当迭代次数趋向无穷时，函数 $\psi(n)-n$ 的迭代无界，最小的这样的数是 $n=318$。

如果求 ϕ 和 ψ 函数之平均 $\frac{1}{2}(\varphi+\psi)$ 再行迭代，只要它们是素数幂，就产生出其项变为常数的序列。例如对 24 有 $\frac{1}{2}(8+48)=28$，$\frac{1}{2}(12+48)=30$，$\frac{1}{2}(8+72)=40$，$\frac{1}{2}(16+72)=44$，$\frac{1}{2}(20+72)=46$，$\frac{1}{2}(22+72)=47$，$\frac{1}{2}(46+48)=47$，…。Charles R. Wall 给出了迭代导致无界序列的例子：从 45，48，…或从 50，55，…开

始，继续下去有 56，60，80，88，92，94，95，96，…. 第 35 项之后的每一项都是它前面倒数第八项的两倍！

我们还可以求 σ 及 φ 函数之平均再作迭代. 由于对 $n>2$，$\varphi(n)$ 恒为偶数，而当 n 为平方数或为一平方数的两倍时，$\sigma(n)$ 是奇数，故有时会得到非整数值. 例如 54，69，70，84，124，142，143，144，$225\frac{1}{2}$. 在此情形我们说该序列**出现断裂**(fracture). 容易证明，仅当 $n=1$ 或为素数时有 $(\sigma(n)+\varphi(n))/2=n$，故序列可能变成常数，例如 60，92，106，107，107，…. 是否存在无限增长又不出现断裂的序列呢？

当然，如果我们对 φ 函数作迭代，最终会得到 1. 称使得 $\varphi^k(n)=1$ 成立的最小整数 k 为 n 的**类**(class).

k	n																	
1											2							
2	3										4	6						
3	5	7									8	9	10	12	14	18		
4	11	13	15								16	19	20	21	22	24	26		…
5	17	23	25	29	31						32	33	34	35	37	39	40	43	…
6	41	47	51	53	55	59	61				64	65	67	68	69	71	73		…
7	83	85	89	97	101	103	107	113	115	119	121	122	123	125	128				

类的最小值的集合是 $M=\{2,3,5,11,17,41,83,\cdots\}$. Shapiro 猜想 M 只包含素数，但 Mills 发现其中有一些合数. 如果 S 是对所有 k，类 k 中 $<2^k$ 的元素之并集，那么

$$S=\{3;5,7;11,13,15;17,23,25,29,31;41,47,51,53,55,59,61;83,85,\cdots\},$$

likewise Shapiro 证明了，S 中元素的因子也在 S 中. Catlin 证明了，如果 m 是 M 中一个奇数，则 M 的因子也在 M 中，且仅当 M 中有有限多个奇数时，M 中才有有限多个素数. S 包含无穷多个奇数吗？M 包含无穷多个奇数吗？

Pillai 证明了，n 的类 $k=k(n)$ 满足

$$\left\lfloor \frac{\ln n}{\ln 3} \right\rfloor \leqslant k(n) \leqslant \left\lfloor \frac{\ln n}{\ln 2} \right\rfloor,$$

且易见(看 $2^a 3^b$)$k(n)/\ln n$ 在区间$[1/\ln 3, 1/\ln 2]$中稠密. $k(n)$的平均性状及正规性状如何? Erdös, Granville, Pomerance 和 Spiro 猜想存在一个常数 α,使 $k(n)$的正规阶是 $\alpha \ln n$,并在假设 Elliott-Halberstam 猜想为真的条件下证明了此猜想. 他们还证明了,对每个正整数 h,$\varphi^h(n)/\varphi^{h+1}(n)$的正规阶是 $he^\gamma \ln\ln\ln n$,这里 γ 是 Euler 常数. 见他们有关许多未解决的问题的论文. 例如,若 $\sigma^k(n)$是因子之和这一函数的第 k 次迭代,他们无法证明或推翻下列任一命题.

¿ 对每个 $n>1$,当 $k\to\infty$时有 $\sigma^{k+1}(n)/\sigma^k(n)\to 1$?

¿ 对每个 $n>1$,当 $k\to\infty$时有 $\sigma^{k+1}(n)/\sigma^k(n)\to\infty$?

¿ 对每个 $n>1$,当 $k\to\infty$时有$(\sigma^k(n))^{1/k}\to\infty$?

¿ 对每个 $n>1$,存在某个 k 使 $n\mid\sigma^k(n)$?

¿ 对每个 $n,m>1$,存在某个 k 使 $m\mid\sigma^k(n)$?

¿ 对每个 $n,m>1$,存在某个 k,l 使 $\sigma^k(m)=\sigma^l(n)$?

Miriam Hausman 刻画了方程 $n=m\varphi^k(n)$的解 n 的特征. 它们主要的特征是形如 $2^a 3^b$.

Finucane 对函数 $\varphi(n)+1$ 作了迭代,并问道:经过多少步可以得到素数? 又给定一个素数 p,那么对终止于 p 的序列来说,n 的值的分布如何? 5,8,10,12 是仅有的终止于 5 的数吗? 而 7,9,14,15,16,18,20,24,30 是仅有的终止于 7 的数吗?

Erdös 对 $\sigma(n)-1$ 的迭代提出了类似的问题. 它永远终止于素数呢,还是它可以无限增长呢? 不论在 $\sigma(n)-1$,$(\psi(n)+\varphi(n))/2$还是$(\varphi(n)+\sigma(n))/2$ 的迭代的情形,他都不能证明其增长比指数来得慢. 有关的结果及猜想,见下面提到的四位作者的论文.

Atanassov 定义了 φ 和 σ 的某些加性类似物,提出了 17 个问题,但只回答了其中 3 个问题.

参考文献

Krassimir T. Atanassov, New integer functions, related to ϕ and σ functions, *Bull. Number Theory Related Topics*, **11**(1987) 3–26; *MR* **90j**:11007.

P. A. Catlin, Concerning the iterated ϕ-function, *Amer. Math. Monthly*, **77**(1970) 60–61.

P. Erdős, A. Granville, C. Pomerance & C. Spiro, On the normal behavior of the iterates of some arithmetic functions, in Berndt, Diamond, Halberstam & Hildebrand (editors), Analytic Number Theory, *Proc. Conf. in honor P.T. Bateman, Allerton Park, 1989*, Birkhäuser, Boston, 1990, 165–204; *MR* **92a**:11113.

P. Erdős, Some remarks on the iterates of the ϕ and σ functions, *Colloq. Math.*, **17**(1967) 195–202; *MR* **36** #2573.

Paul Erdős & R. R. Hall, Euler's ϕ-function and its iterates, *Mathematika*, **24**(1977) 173–177; *MR* **57** #12356.

Miriam Hausman, The solution of a special arithmetic equation, *Canad. Math. Bull.*, **25**(1982) 114–117.

W. H. Mills, Iteration of the ϕ-function, *Amer. Math. Monthly*, **50**(1943) 547–549; *MR* **5**, 90.

C. A. Nicol, Some diophantine equations involving arithmetic functions, *J. Math. Anal. Appl.*, **15**(1966) 154–161.

Ivan Niven, The iteration of certain arithmetic functions, *Canad. J. Math.*, **2**(1950) 406–408; *MR* **12**, 318.

S. S. Pillai, On a function connected with $\phi(n)$, *Bull. Amer. Math. Soc.*, **35**(1929) 837–841.

Carl Pomerance, On the composition of the arithmetic functions σ and ϕ, *Colloq. Math.*, **58**(1989) 11–15; *MR* **91c**:11003.

Harold N. Shapiro, An arithmetic function arising from the ϕ-function, *Amer. Math. Monthly*, **50**(1943) 18–30; *MR* **4**, 188.

Charles R. Wall, Unbounded sequences of Euler-Dedekind means, *Amer. Math. Monthly*, **92**(1985) 587.

B42. $\varphi(\sigma(n))$和$\sigma(\varphi(n))$的性状

Erdös要求我们证明：对几乎所有 n 有 $\varphi(n)>\varphi(n-\varphi(n))$，但对无穷多个 n 有 $\varphi(n)<\varphi(n-\varphi(n))$.

Mąkowski 和 Schinzel 证明了

$$\limsup \varphi(\sigma(n))/n=\infty, \quad \limsup \varphi^2(n)/n=\frac{1}{2}$$

以及 $\liminf \sigma(\varphi(n))/n \leqslant \frac{1}{2}+\frac{1}{2^{34}-4}$. 他们问：对所有 n 是否有

$\sigma(\varphi(n))/n \geq \frac{1}{2}$? 他们指出,即使 $\inf \sigma(\varphi(n))/n > 0$ 也没有得到证明,但 Pomerance 用 Brun 的方法证明了它.

John Selfridge, Fred Hoffman 和 Rich Schroeppel 找到了 $\varphi(\sigma(n)) = n$ 的 24 个解,即

2^k(对 $k=0,1,3,7,15$ 和 31);$2^2\cdot3$;$2^8\cdot3^3$;$2^{10}\cdot3^3\cdot11^2$;$2^{12}\cdot3^3\cdot5\cdot7\cdot13$;$2^4\cdot3\cdot5$;$2^4\cdot3^2\cdot5$;$2^9\cdot3\cdot5^2\cdot31$;$2^9\cdot3^2\cdot5^2\cdot31$;$2^5\cdot3^4\cdot5\cdot11$;$2^5\cdot3^4\cdot5^2\cdot11$;$2^8\cdot3^4\cdot5\cdot11$;$2^8\cdot3^4\cdot5^2\cdot11$;$2^5\cdot3^6\cdot7^2\cdot13$;$2^6\cdot3^6\cdot7^2\cdot13$;$2^{13}\cdot3^7\cdot5\cdot7^2$;$2^{13}\cdot3^7\cdot5^2\cdot7^2$;$2^{21}\cdot3^3\cdot5\cdot11^3\cdot31$;$2^{21}\cdot3^3\cdot5^2\cdot11^3\cdot31$.

当然,对应也有 $\sigma(\varphi(m)) = m$ 的 24 个解.问题是还有其他的解吗?有无穷多个解吗?

Golomb 注意到,如果 $q>3$ 和 $p=2q-1$ 是素数,且 $m\in\{2,3,8,9,15\}$,那么 $n=pm$ 是 $\varphi(\sigma(n))=\varphi(n)$的一个解.无疑有无穷多个这样的解,且毫无疑问在可见的将来无人能证明此结论.它还有其他的解 1, 3, 15, 45, …;它有无穷多个解吗?他给出 $\sigma(\varphi(n))=\sigma(n)$的解 1,87,362,1257,1798,5002,9374.他还注意到,如果 p 和$(3^p-1)/2$ 是素数(例如 $p=3,7,13,71,103$),那么 $n=3^{p-1}$是 $\sigma(\varphi(n))=\varphi(\sigma(n))$的解.他还证明了 $\sigma(\varphi(n))-\varphi(\sigma(n))$ 无穷多次取正的值和负的值.他问道:每种情形所占的比例如何?

参考文献

P. Erdős, Problem P. 294, *Canad. Math. Bull.*, **23**(1980) 505.

Solomon W. Golomb, Equality among number-theoretic functions, preprint, Oct 1992; Abstract 882-11-16, *Abstracts Amer. Math. Soc.*, 14(1993) 415–416.

A. Mąkowski & A. Schinzel, On the functions $\phi(n)$ and $\sigma(n)$, *Colloq. Math.*, 13(1964–65) 95–99; *MR* **30** #3870.

Carl Pomerance, On the composition of the arithmetic functions σ and ϕ, *Colloq. Math.*, **58**(1989) 11–15; *MR* **91c**:11003.

József Sándor, On the composition of some arithmetic functions, *Studia Univ. Babeş-Bolyai Math.*, **34**(1989) 7–14; *MR* **91i**:11008.

B43. 阶乘的交错和

诸数

$$3!-2!+1!=5,$$
$$4!-3!+2!-1!=19,$$
$$5!-4!+3!-2!+1!=101,$$
$$6!-5!+4!-3!+2!-1!=619,$$
$$7!-6!+5!-4!+3!-2!+1!=4421,$$
$$8!-7!+6!-5!+4!-3!+2!-1!=35899$$

均为素数.有无穷多个这样的数吗？下面的表给出对于在它们后面的几个 n 的值，$A_n=n!-(n-1)!+(n-2)!-+\cdots-(-1)^n1!$ 的因子：

n	A_n	n	A_n
9	79·4139	19	1155787176220229 81(prime)
10	3301819(prime)	20	8969·210101·1229743351
11	13·2816537	21	113·167·4511191·572926421
12	29·15254711	22	79·239·56947572104043899
13	47·1427·86249	23	85439·289993909455734779
14	211·1679·229751	24	12203·24281·2010359484638233
15	1226280710981(prime)	25	59·555307·455254005662640637
16	53·6581·56470483	26	1657·234384986539153832538067
17	47·7148742955723	27	127^2·271·1163·20656334799701305 93
18	2683·2261044646593	28	61·221171·21820357757749410439949

例子 $n=27$ 表明这些数未必是无平方因子数. Wilfrid Keller 继续计算到 $n\leqslant 335$. 对 $n=41,59,61,105$ 及 160, A_n 是素数.

如果有 n 的值使 $n+1$ 整除 A_n，那么对所有 $m>n$，$n+1$ 也整除 A_m，于是它只能有有限多个素数值. Wagstaff 证明了，如果有这样一个 n 存在，它必大于 46340.

B44. 阶乘的和

D. Kurepa 定义 $!n = 0! + 1! + 2! + \cdots + (n-1)!$，并问是否对所有 $n > 2$ 有 $!n \not\equiv 0 \bmod n$? Slavić 对 $3 \leqslant n \leqslant 1000$ 用计算机对此作了验证. 人们猜想 $(!n, n!) = 2$. Wagstaff 将对此猜想的计算和验证扩大到 $n < 50000$. Mijajlović 则对 $n \leqslant 10^6$ 进行了验证. 他注意到，对 $K_n = !(n+1) - 1 = 1! + 2! + \cdots + n!$ 我们有如下结论：对 $n \geqslant 2$ 有 $3 | K_n$；对 $n \geqslant 5$ 有 $9 | K_n$；而对 $n \geqslant 10$ 则有 $99 | K_n$. Wilfrid Keller 一直从事进一步的计算和验证，他对 $n < 10^6$ 没有发现 K_n 有任何新的整除性. 在一封 1991 年 3 月 21 日的信中，Reg. Bond 对此猜想给出一个未经发表的证明.

又猜想除了 2^2 整除 $!3$ 外，$!n$ 是无平方因子数. Mijajlović 证实了对 $m \leqslant 1223$ 有 $m^2 \nmid !n$.

参考文献

L. Carlitz, A note on the left factorial function, *Math. Balkanika*, **5**(1975) 37–42.

Đuro Kurepa, On some new left factorial propositions, *Math. Balkanika*, **4**(1974) 383–386; *MR* **58** #10716.

Ž. Mijajlović, On some formulas involving $!n$ and the verification of the $!n$-hypothesis by use of computers, *Publ. Inst. Math.* (*Beograd*) (*N.S.*) **47(61)** (1990) 24–32; *MR* **92d**:11134.

B45. Euler 数

展开式 $\sec x = \sum E_n (ix)^n / n!$ 中的系数即为 **Euler 数**(Euler number)，它是在许多组合问题中提出来的. $E_0 = 1, E_2 = -1, E_4 = 5, E_6 = -61, E_8 = 1385, E_{10} = -50521, E_{12} = 2702765, E_{14} = -199360981, E_{16} = 19391512145, E_{18} = -2404879675441, \cdots$. 对任何素数 $p \equiv 1 \bmod 8$, $E_{(p-1)/2} \not\equiv 0 \bmod p$ 是否为真? 它对 $p \equiv 5 \bmod 8$ 是否为真?

参考文献

E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, *Annals of Math.* **39**(1938) 350–360; *Zbl.* **19**, 5.

Barry J. Powell, Advanced problem 6325, *Amer. Math. Monthly*, **87**(1980) 826.

B46. n 的最大素因子

Erdös 用 $P(n)$ 记 n 的最大素因子，并问是否有无穷多个素数 p 使 $(p-1)/P(p-1)=2^k$ 或 $=2^k\cdot 3^l$？

如果 $n>2$，则 $P(n)$，$P(n+1)$，$P(n+2)$ 全不相同．证明 {低，中，高} 的 6 个排列中的每一个都出现无穷多次，且以同样的频率出现．$2^k-2,2^k-1,2^k$ 表明：中、高、低对无穷多个 k 都出现，这是因为由 Bang(或 Mahler) 的一个定理，当 $k\to\infty$ 时有 $P(2^k-1)\to\infty$．为了看出低、中、高出现无穷多次，我们要问对素数 p 来说，$p-1$，p 和 $p+1$ 是否能获得成功？答曰不行！试用 p^2-1，p^2 以及 p^2+1 或许可以．如果 $P(p^2+1)<p$，可以试用 p^4-1，p^4 和 p^4+1．说到底，对每个素数 p，都会有一个 k 的值使 $P(p^{2^k}+1)>p$．

Selfridge 对 2^k，2^k+1 和 2^k+2 解决了低、高、中的情形，而 Tijdeman 对中、低、高情形给出如下的讨论：考虑下述可能性 $2^k-1,2^k,2^k+1;2^{2k}-1,2^{2k},2^{2k}+1;2^{4k}-1,2^{4k},2^{4k}+1;\cdots$．

参考文献

P. Erdös & Carl Pomerance, On the largest prime factors of n and $n+1$, *Aequationes Math.*, **17**(1978) 311–321; *MR* **58** #476.

B47. 何时 2^a-2^b 整除 n^a-n^b？

Selfridge 注意到：对所有 n，2^2-2 整除 n^2-n，$2^{2^2}-2^2$ 整除

$n^{2^2}-n^2$，$2^{2^{2^2}}-2^{2^2}$ 整除 $n^{2^{2^2}}-n^{2^2}$. 他问：对什么样的 a 和 b，2^a-2^b 能整除 n^a-n^b（对所有 n）？$n=3$ 的情形由 Harry Ruderman 在 *Amer. Math. Monthly*, 81(1974) 405 上作为问题 E2468* 提了出来. 在解答中(83(1976) 288－289)Bill Vélez 把$(b,a-b)=(0,1)$作为平凡解予以省略，并给出另外 13 个解：(1,1)，(1,2)，(2,2)，(3,2)，(1,4)，(2,4)，(3,4)，(4,4)，(2,6)，(3,6)，(2,12)，(3,12)，(4,12). 由 Pomerance 所做的评论(84(1977) 59－60)表明，Schinzel 的结果完成了 Vélez 的解. 孙琦(Sun Qi)和张明志(Zhang Ming-Zhi)也对此问题作了解答.

参 考 文 献

A. Schinzel, On primitive prime factors of a^n-b^n, *Proc. Cambridge Philos. Soc.*, **58**(1962) 555–562.

Sun Qi & Zhang Ming-Zhi, Pairs where 2^a-2^b divides n^a-n^b for all n, *Proc. Amer. Math. Soc.*, **93**(1985) 218–220; *MR* **86c**:11004.

B48. 经过素数的乘积

David Silverman 注意到，如果 p_n 是第 n 个素数，则

$$\prod_{n=1}^{m}\frac{p_n+1}{p_n-1}$$

对 $m=1,2,3,4$ 和 8 都是整数. 他问它还能再取整数吗？等价地说，正如 Mąkowski 所看到的(见问题 B16 的文献)，就是问对什么样的 $n=\prod_{r=1}^{m}p_r$，$\varphi(n)$整除 $\sigma(n)$？例如，如果 $\sigma(n)=4\varphi(n)$，那么 $2n$ 或者是一个完全数，或者是一个过剩数，即有 $\sigma(2n)\geq 4n$.

Wagstaff 要求对

$$\prod\frac{p^2+1}{p^2-1}=\frac{5}{2}$$

给出一个初等证明(比方说不用 Riemannζ 函数的性质)，这里的乘积经过所有素数. 看起来不大可能有一个不用解析方法的证明.

乍一看似乎诸分数可以相消，但是没有哪个分子能被 3 整除. Euler 的证明是

$$\prod \frac{p^2+1}{p^2-1} = \prod \frac{p^4-1}{(p^2-1)^2} = \prod \frac{1-p^{-4}}{(1-p^{-2})^2}$$

$$= \frac{\zeta^2(2)}{\zeta(4)} = \frac{(\pi^2/6)^2}{\pi^4/90} = \frac{5}{2}.$$

这里用到 $\sum n^{-k} = \prod (1-p^{-k})^{-1}$, $\sum n^{-2} = \pi^2/6$ 以及 $\sum n^{-4} = \pi^4/90$. Wagstaff 认为第一式是初等的，但后两个不是. 他希望看到 $2\left(\sum n^{-2}\right)^2 = 5\sum n^{-4}$ 或者

$$4\sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{m=n+1}^{\infty} \frac{1}{m^2} = 3\sum \frac{1}{n^4}$$

的一个直接证明.

B49. Smith 数

Albert Wilansky 从他姐夫的电话号码

$$4937775 = 3\cdot5\cdot5\cdot65837$$

想到把各位数字之和等于它的所有素因子的各位数字之和的数称为 **Smith 数**(Smith number)，这种数很快吸引了大家的兴趣. 平凡地说，任何素数皆是 Smith 数，而 4, 22, 27, 58, 85, 94, 121, … 也都是 Smith 数. Oltikar 和 Wayland 给出例子 $3304(10^{317}-1)/9$ 和 $2\cdot10^{45}(10^{317}-1)/9$，而寻找越来越大的 Smith 数的竞赛仍在继续. Yates 给出有 10694985 位数字的 Smith 数

$$10^{3913210}(10^{1031}-1)(10^{4594}+3\cdot10^{2297}+1)^{1476},$$

从那以后，他又用一个有 13614513 位数字的 Smith 数打破了他自己的记录.

参考文献

Stephen K. Doig, Math Whiz makes digital discovery, *The Miami Herald*, 1986-08-22; *Coll. Math. J.*, **18**(1987) 80.

Editorial, Smith numbers ring a bell? *Fort Lauderdale Sun Sentinel*, 86-09-16, p. 8A.

Editorial, Start with 4,937,775, *New York Times*, 86-09-02.

Wayne L. McDaniel, The existence of infinitely many k-Smith numbers, *Fibonacci Quart.*, **25**(1987) 76–80.

Wayne L. McDaniel, Powerful k-Smith numbers, *Fibonacci Quart.*, **25**(1987) 225–228.

Wayne L. McDaniel, Palindromic Smith numbers, *J. Recreational Math.*, **19**(1987) 34–37.

Wayne L. McDaniel, Difference of the digital sums of an integer base b and its prime factors, *J. Number Theory*, **31**(1989) 91–98; *MR* **90e**:11021.

Wayne L. McDaniel & Samuel Yates, The sum of digits function and its application to a generalization of the Smith number problem, *Nieuw Arch. Wisk.*(4), **7**(1989) 39–51.

Sham Oltikar & Keith Wayland, Construction of Smith numbers, *Math. Mag.*, **56**(1983) 36–37.

Ivars Peterson, In search of special Smiths, *Science News*, 86-08-16, p. 105.

A. Wilansky, Smith numbers, *Two-Year Coll. Math. J.*, **13**(1982) 21.

Samuel Yates, Special sets of Smith numbers, *Math. Mag.*, **59**(1986) 293–296.

Samuel Yates, Smith numbers congruent to 4 (mod 9), *J. Recreational Math.*, **19**(1987) 139–141.

Samuel Yates, How odd the Smith are, *J. Recreational Math.*, 19(1987) 168–174.

Samuel Yates, Digital sum sets, in R. A. Mollin (ed.), Number Theory, *Proc. 1st Canad. Number Theory Assoc. Conf., Banff, 1988*, de Gruyter, New York, 1990, pp. 627–634; *MR* **92c**:11008.

Samuel Yates, Tracking titanics, in R. K. Guy & R. E. Woodrow (eds.), The Lighter Side of Mathematics, *Proc. Strens Mem. Conf., Calgary, 1986*, Spectrum Series, Math. Assoc. of America, Washington DC, 1994.

C. 堆垒数论

C1. Goldbach 猜想

最为名声显赫的问题之一是 Goldbach 猜想：每个大于 4 的偶数可表为两个奇素数之和. Javier Echevarria 对直到 2^{32}的偶数作了验证，Matti Sinisalo 验证到 4×10^{11}. Vinogradov 证明了每个大于 $3^{3^{15}}$(事实上做出这一成果的应是 K. G. Borozdkin，他用 Vinogradov 方法得到的界是 $e^{e^{16.038}}$——译者注)的奇数是三个素数之和. 而陈景润(Chen Jing-Run)则证明了，所有充分大的偶数是一个素数和一个至多是两个素数乘积的数之和. 陈景润和王天泽(Wang Tian-Ze)还将数 $3^{3^{15}}$减小为 $e^{e^{11.503}}$.

Hardy 和 Littlewood 的"猜想 A"(参见 A1，A8)是说：偶数 n 表为二素数之和的表法数 $N_2(n)$渐近地由

$$N_2(n)\sim\frac{2cn}{(\ln n)^2}\prod\left(\frac{p-1}{p-2}\right)$$

给出，这里如在 A8 中一样有 $2c\approx1.3203$，且该乘积取过 n 的所有奇素因子.

M. L. Stein 和 P. R. Stein 对 $n<10^5$ 计算了 $N_2(n)$，并对所有 $k<1911$ 找到了使 $N_2(n)=k$ 成立的 n 的值. 猜想 $N_2(n)$ 取到所有的正整数值. 他们还对 $n<10^8$ 验证了这一猜想. Granville, van de Lune 和 te Riele 将此范围扩大到了 $2\cdot10^{10}$.

设 $\varphi(n)$是 Euler φ 函数(B36)，故若 p 为素数则有 $\varphi(p)=p-1$. 如果 Goldbach 猜想为真，则对每个数 m 存在素数 p, q 使得

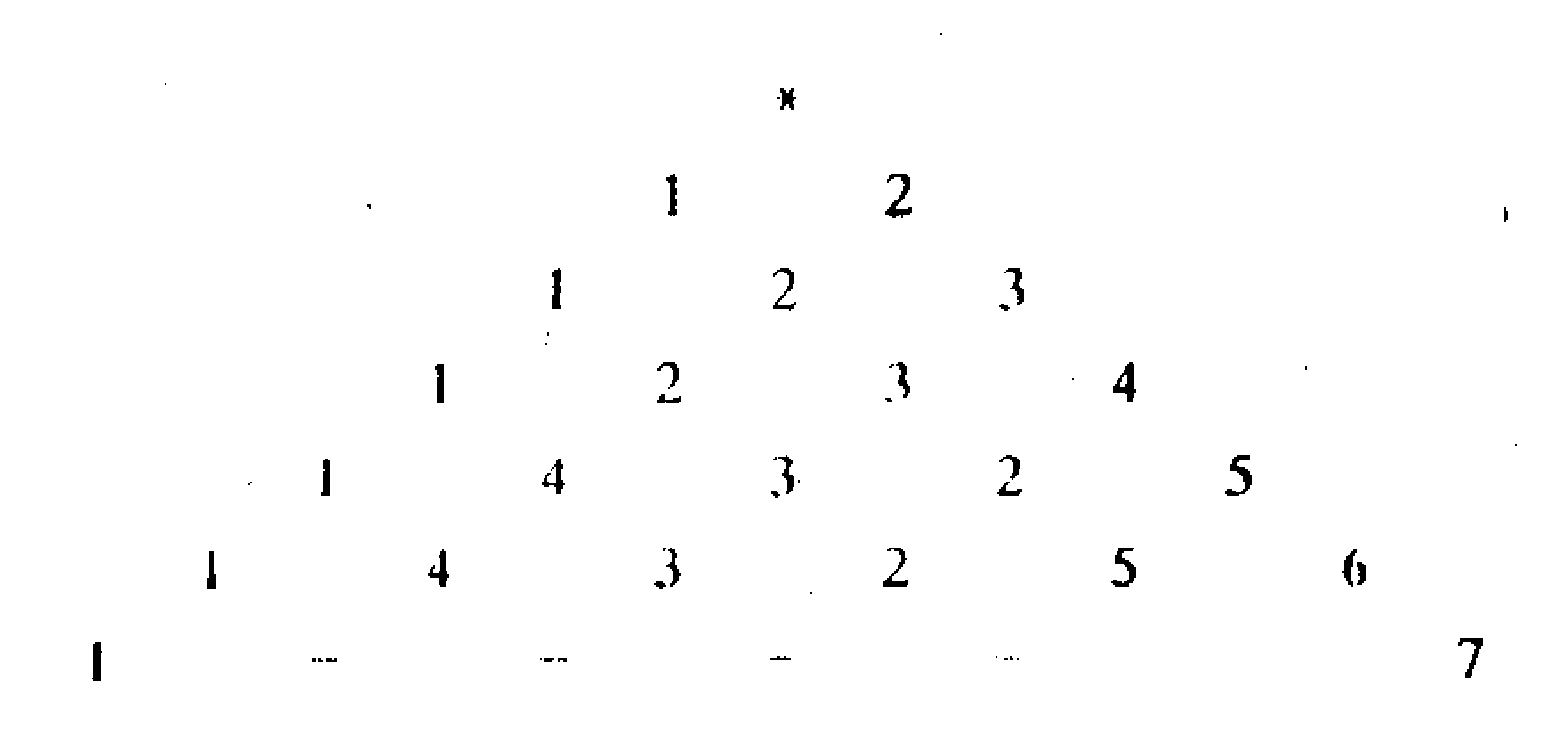
$$\varphi(p)+\varphi(q)=2m.$$

如果将 p 和 q 为素数这一条件放宽，则证明恒有满足此方程的数

p 和 q 存在应较为容易. Erdös 和 Leo Moser 问它是否能得到证明?

Antonio Filz 定义阶为 $2m$ 的一个素圈(prime circle)是从 1 到 $2m$ 的数的一个环形排列,其中每一对相邻数之和均为素数. 对 $m=1,2,3$ 本质上只有一个素圈,对 $m=4$ 有两个素圈,而对 $m=5$ 有 48 个. 是否对所有 m 都有素圈存在? 给出素圈个数的一个渐近估计.

类似地,Margaret Kenney 提出素金字塔(prime pyramid)



其中第 n 行包含数 $1,2,\cdots,n$(从 1 开始,以 n 结束),每两个相邻数的和皆为素数. 在第 n 行中可以用多少种方式放置这些数? 这个问题是由 Morris Wald 提出来的. 给出的解几乎肯定总是成功的,但是给出它的证明可能和证明 Goldbach 猜想本身同样困难. E. T. H. Wang 早些时候提出一个限制条件较弱的问题:对接尾的数事先不予指定.

Erdös 问是否有无穷多个素数 p 存在,使得每个 $\leqslant p-3$ 的偶数均可表为两个都 $\leqslant p$ 的素数之差? 例如, $p=13$: $10=13-3$, $8=11-3$, $6=11-5$, $4=7-3$, $2=5-3$.

参考文献

J. Bohman & C.-E. Froberg, Numerical results on the Goldbach conjecture, *BIT*, **15**(1975) 239–243.

Chen Jing-Run, On the representation of a large even number as the sum of a

prime and the product of at most two primes, *Sci. Sinica*, **16**(1973) 157–176; *MR* **55** #7959; II, **21**(1978) 421–430; *MR* **80e**:10037.

Chen Jing-Run & Wang Tian-Ze, On the Goldbach problem (Chinese), *Acta Math. Sinica*, **32**(1989) 702–718; *MR* **91e**:11108.

J. G. van der Corput, Sur l'hypothèse de Goldbach pour presque tous les nombres pairs, *Acta Arith.*, **2**(1937) 266–290.

N. G. Čudakov, On the density of the set of even numbers which are not representable as the sum of two odd primes, *Izv. Akad. Nauk SSSR Ser. Mat.*, **2**(1938) 25–40.

N. G. Čudakov, On Goldbach-Vinogradov's theorem, *Ann. Math.*(2), **48** (1947) 515–545; *MR* **9**, 11.

Jean-Marc Deshouillers, Andrew Granville, Wladyslaw Narkiewicz & Carl Pomerance, An upper bound in Goldbach's problem, *Math. Comput.*, **61**(1993) 209–213.

T. Estermann, On Goldbach's problem: proof that almost all even positive integers are sums of two primes, *Proc. London Math. Soc.*(2), 44(1938) 307–314.

Antonio Filz, Problem 1046, *J. Recreational Math.*, 14(1982) 64; **15**(1983) 71.

D. A. Goldston, Linnik's theorem on Goldbach numbers in short intervals, *Glasgow Math. J.*, **32**(1990) 285–297; *MR* **91i**:11134.

A. Granville, J. van de Lune & H. J. J. te Riele, Checking the Goldbach conjecture on a vector computer, in R. A. Mollin (ed.), Number Theory and Applications, NATO ASI Series, Kluwer, Boston, 1989, pp. 423–433; *MR* **93c**:11085.

Richard K. Guy, Prime Pyramids, *Crux Mathematicorum*, **19**(1993) 97–99.

Margaret J. Kenney, Student Math Notes, *NCTM News Bulletin*, Nov. 1986.

H. L. Montgomery & R. C. Vaughan, The exceptional set in Goldbach's problem, *Acta Arith.*, **27**(1975) 353–370.

Pan Cheng-Dong, Ding Xia-Xi & Wang Yuan, On the representation of every large even integer as the sum of a prime and an almost prime, *Sci. Sinica*, **18**(1975) 599–610; *MR* **57** #5897

A. Perelli & J. Pintz, On the exceptional set for Goldbach's problem in short intervals, *J. London Math. Soc.*, **47**(1993) 41–49; *MR* **93m**:11104.

P. M. Ross, On Chen's theorem that every large even number has the form $p_1 + p_2$ or $p_1 + p_2p_3$, *J. London Math. Soc.*(2), **10**(1975) 500–506.

Matti K. Sinisalo, Checking the Goldbach conjecture up to $4 \cdot 10^{11}$, *Math. Comput.*, **61**(1993) 931–934.

M. L. Stein & P. R. Stein, New experimental results on the Goldbach conjecture, *Math. Mag.*, **38**(1965) 72–80; *MR* **32** #4109.

M. L. Stein & P. R. Stein, Experimental results on additive 2-bases, *Math. Comput.*, **19**(1965) 427–434.

Robert C. Vaughan, On Goldbach's problem, *Acta Arith.*, **22**(1972) 21–48.

Robert C. Vaughan, A new estimate for the exceptional set in Goldbach's problem, *Proc. Symp. Pure Math.*, (Analytic Number Theory, St. Louis), Amer. Math. Soc., **24**(1972) 315–319.

I. M. Vinogradov, Representation of an odd number as the sum of three primes,

Dokl. Akad. Nauk SSSR, **15**(1937) 169–172.
I. M. Vinogradov, Some theorems concerning the theory of primes, *Mat. Sb. N.S.*, **2**(**44**) (1937) 179–195.
Morris Wald, Problem 1664, *J. Recreational Math.*, **20**(1987–88) 227–228; Solution **21**(1988–89) 236–237.
Edward T. H. Wang, Advanced Problem 6189, *Amer. Math. Monthly*, **85** (1978) 54 [no solution has appeared].
Wang Yuan (editor), *Goldbach Conjecture*, World Scientific, Singapore, 1984. [A collection of original papers, translated into English when other languages were used, with a 15-page Introduction.]
Dan Zwillinger, A Goldbach conjecture using twin primes, *Math. Comput.*, **33** (1979) 1071; *MR* **80b**:10071.

C2. 相连素数和

令 $f(n)$ 为 n 表示成(一个或多个)相连素数之和的表法数. 例如

$$5=2+3 \quad 以及 \quad 41=11+13+17=2+3+5+7+11+13,$$

故有 $f(5)=2$ 及 $f(41)=3$. Leo Moser 证明了

$$\lim_{x\to\infty}\frac{1}{x}\sum_{n=1}^{x}f(n) = \ln 2,$$

并问是否无穷多次有 $f(n)=1$? 对每个 k, $f(n)=k$ 是否都可解? 对每个 k, 使 $f(n)=k$ 成立的数有密度吗? 是否有 $\limsup f(n)=\infty$?

Erdös 问是否有无穷整数序列 $1<a_1<a_2<\cdots$, 使 $a_i+a_{i+1}+\cdots+a_k=n$ 的解数 $f(n)$ 与 n 一道趋向无穷? 他注意到, 如果强调要 $k>i$, 那么甚至还不知道对除了有限多个数以外的所有的 n, 是否有 $f(n)>0$. 如果 $a_i=i$, $f(n)$ 就是 n 的奇因子个数.

参考文献

L. Moser, Notes on number theory III. On the sum of consecutive primes, *Canad. Math. Bull.*, **6**(1963) 159–161; *MR* **28** #75.

C3. 幸 运 数

Gardiner 和其他人根据修改的 Eratosthenes 筛法，用下述方式定义了幸运数(lucky number). 从自然数中剔出所有偶数，留下奇数. 除了 1 以外，第一个留下的数是 3. 在新数列中每 3 个数去掉一个数(即去掉那些形如 $6k-1$ 的数)，剩下的是

$$1,3,7,9,13,15,19,21,25,27,31,33,\cdots$$

下一个留下的数是 7，在该数列中每 7 个数去掉一个数(即去掉那些形如 $42k-23$ 和 $42k-3$ 的数). 再下一个剩下的数是 9，再从剩下的数列中每 9 个数去掉一个数，如此一直做下去，直到最后得到幸运数

1,3,7,9,13,15,21,25,31,33,37,43,49,51,63,67,69,
73,75,79,87,93,99,105,111,115,127,129,133,135,141,
151,159,163,169,171,189,193,195,201,205,211,219,223,
231,…

与有关素数的经典问题相平行地，人们对幸运数也提出许多问题. 例如，若 $L_2(n)$ 是 $l+m=n$ 的解数，这里 n 是偶数而 l 和 m 是幸运数，则 M. L. Stein 和 P. R. Stein 找到了 n 的值，使对所有 $k\leqslant 1769$ 有 $L_2(n)=k$，又对 C1 中所做的猜想有一个对应的猜想.

参考文献

W. E. Briggs, Prime-like sequences generated by a sieve process, *Duke Math. J.*, **30**(1963) 297–312; *MR* **26** #6145.

R. G. Buschman & M. C. Wunderlich, Sieve-generated sequences with translated intervals, *Canad. J. Math.*, **19**(1967) 559–570; *MR* **35** #2855.

R. G. Buschman & M. C. Wunderlich, Sieves with generalized intervals, *Boll. Un. Mat. Ital.*(3), **21**(1966) 362–367.

Paul Erdős & Eri Jabotinsky, On sequences of integers generated by a sieving process, I, II, *Nerderl. Akad. Wetensch. Proc. Ser. A*, **61** = *Indag. Math.*, **20**(1958) 115–128; *MR* **21** #2628.

Verna Gardiner, R. Lazarus, N. Metropolis & S. Ulam, On certain sequences of

integers generated by sieves, *Math. Mag.*, **31**(1956) 117–122; **17**, 711.
David Hawkins & W. E. Briggs, The lucky number theorem, *Math. Mag.*, **31**(1957–58) 81–84, 277–280; *MR* **21** #2629, 2630.
M. C. Wunderlich, Sieve-generated sequences, *Canad. J. Math.*, **18**(1966) 291–299; *MR* **32** #5625.
M. C. Wunderlich, A general class of sieve generated sequences, *Acta Arith.*, **16**(1969–70) 41–56; *MR* **39** #6852.
M. C. Wunderlich & W. E. Briggs, Second and third term approximations of sieve-generated sequences, *Illinois J. Math.*, **10**(1966) 694–700; *MR* **34** #153.

C4. Ulam 数

Ulam 从任意的 u_1 和 u_2 开始，继之以恰好以惟一方式用前面某两个不同的数的和表出之数，如此他构造出递增的正整数序列．Recamán 问了一些与 U-数（U-number，即 Ulam 数——译者注）($u_1=1, u_2=2$)

1,2,3,4,6,8,11,13,16,18,26,28,36,38,47,48,53,57
62,69,72,77,82,87,97,99,102,106,114,126,131,138,145,
148,155,175,177,180,182,189,197,206,209,219,…

有关的问题：

(1)除了 $1+2=3$ 以外，两个相邻的 U-数之和能是一个 U-数吗？

(2)有无穷多个数

23,25,33,35,43,45,67,92,94,96,…

不是两个 U-数之和吗？

(3)(Ulam)U-数有正密度吗？

(4)有无穷多对相邻的 U-数

(1,2),(2,3),(3,4),(47,48),…

吗？

(5)U-数序列中有任意大的间隙吗？

为了回答问题(1)，Frank Owens 注意到 $u_{19}+u_{20}=62+69=131=u_{31}$．为了回答问题(4)，Muller 计算了 20000 项，但未找到新的例子．另一方面，有多于 60% 的项与另一个项的差恰好是 2．

David Zeitlin 问 U-数的序列是否是完全的(complete),这里序列的完全性是指每个正数均可表为该序列中不同元素之和. Stefan Burr 注意到此结论为真,因为 2 以后的每一项都小于它前一项的两倍.

要提醒读者的是,在与 Alan Baker 对"S-数"和"T-数"的刻画有关的代数数论中,Mahler 也曾用到"U-数"这一名词.

更一般地,我们可以定义用同样的方式构造出来的 s-加性序列(s-additive sequence):除了每一项恰可用 s 种方式表为它前面某两项之和外,其余与前定义相同. U-数对应于 $s=1$. 如果 $s=0$,序列是从不是前面两个不同的数之和的数构造出来的. 与下面的问题 C9,E28 和 E32 相比较. 更一般地还有所谓的(s,t)-加性序列((s,t)-additive sequence),这个序列里的每一项恰好可以用 s 种方式表示成前面某 t 个不同的元素之和. 用这个记号,U-数正是从 $u_1=1,u_2=2$ 开始的$(1,2)$-加性序列. Steven Finch 在这方面做了许多工作,并有一些猜想. 例如,从(u_1,u_2)($u_1<u_2$,$u_1\perp u_2$)开始的序列在下列情形只包含有限多个偶数项:(a)$(u_1,u_2)=(2,u_2)$(对 $u_2\geqslant 5$);(b)$(4,u_2)$;(c)$(5,6)$;(d)$u_1\geqslant 6$ 且为偶数;(e)$u_1\geqslant 7$ 为奇数,u_2为偶数. 而在其他情形序列中有无穷多个偶数项.

参考文献

Steven R. Finch, Conjectures about s-additive sequences, *Fibonacci Quart.*, **29**(1991) 209–214; *MR* **92j**:11009.

Steven R. Finch, Are 0-additive sequences always regular? *Amer. Math. Monthly*, **99** (1992) 671–673.

Steven R. Finch, On the regularity of certain 1-additive sequences, *J. Combin. Theory Ser. A*, **60**(1992) 123–130; *MR* **93c**:11009.

Steven R. Finch, Patterns in 1-additive sequences, *Experiment. Math.*, **1** (1992) 57–63; *MR* **93h**11014.

P. Muller, M.Sc. thesis, University of Buffalo, 1966.

Raymond Queneau, Sur les suites s-additives, *J. Combin. Theory*, **12**(1972) 31–71; *MR* **46** #1741.

Bernardo Recamán, Questions on a sequence of Ulam, *Amer. Math. Monthly*, **80**(1973) 919–920.

S. M. Ulam, *Problems in Modern Mathematics*, Interscience, New York, 1964, p. ix.
Marvin C. Wunderlich, The improbable behaviour of Ulam's summation sequence, in *Computers and Number Theory*, Academic Press, 1971, 249–257.

C5. 确定一个集合的元素的和

Leo Moser 提出下列问题，而 Selfridge, Straus 和其他人则大部分予以解决：一个集合中所有数对的和在多大程度上确定该集合？他们证明了：如果这集合的基数不是 2 的幂，则集合的元素可以被确定. 设 $y_1, y_2, \cdots, y_s$ 是诸数 $x_1, x_2, \cdots, x_{2^k}$ 的和 $x_i + x_j (i \neq j)$，那么 $s = 2^{k-1}(2^k - 1)$. 是否有多于两个集合 $\{x_i\}$ 能给出相同的集合 $\{y_j\}$ 呢？如果 $k = 3$，则可能有 3 个这样的集合，例如

$$\{\pm 1, \pm 9, \pm 15, \pm 19\}, \{\pm 2, \pm 6, \pm 12, \pm 22\},$$
$$\{\pm 3, \pm 7, \pm 13, \pm 21\},$$

但是不能有多于 3 个. 对于 $k > 3$ 问题没有解决. 对应于一给定集合的 3 个元素之和的问题，除了以下两种情形外，均已获得解决：如果 $n = 27$ 或 $n = 486$，集合 $\{x_1, x_2, \cdots, x_n\}$ 的 3 个不同元素之和能确定该集合吗？对应于 4 个不同元素和的问题已被 Ewell 解决.

参考文献

John A. Ewell, On the determination of sets by sets of sums of fixed order, *Canad. J. Math.*, **20**(1968) 596–611.
B. Gordon, A. S. Fraenkel & E. G. Straus, On the determination of sets by the sets of sums of a certain order, *Pacific J. Math.*, **12**(1962) 187–196; *MR* **27** #3576.
J. L. Selfridge & E. G. Straus, On the determination of numbers by their sums of a fixed order, *Pacific J. Math.*, **8**(1958) 847–856; *MR* **22** #4657.

C6. 加法链，Brauer 链，Hansen 链

对 n 的一个加法链(addition chain)是一个序列 $1 = a_0 < a_1 <$

$\cdots < a_r = n$，从第二项起每个数都是前面某两个(不一定不同的)元素之和. 例如

$$1,\ 1+1, 2+2, 4+2, 6+2, 8+6$$

以及

$$1, 1+1, 2+2, 4+2, 4+4, 8+6$$

都是对 14 的长度(length)为 $r=5$ 的加法链. 对 n 的加法链的最小长度记为 $l(n)$.

主要的未解决的问题是 Scholz 猜想

$$¿\quad l(2^n-1) \leqslant n-1+l(n) \quad ?$$

对 $n=2^a, 2^a+2^b, 2^a+2^b+2^c, 2^a+2^b+2^c+2^d$，Utz, Gioia 等人给出了证明；对 $1 \leqslant n \leqslant 18$ 则由 Knuth 和 Thurber 给出了证明. Brauer 对存在最短链的那些 n 证明了此猜想，最短链也称为 Brauer 链(Brauer chain)，其中每一个数都用上一个数作为加数. 上面的第二个例子不是 Brauer 链，因为其中的项 4+4 没有用到加数 6. 这样的 n 称为一个 Brauer 数(Brauer number). Hansen 证明了有无穷多个非 Brauer 数，但他还证明了：如果 n 有一个是 Hansen 链的最短链，则 Scholz 猜想仍然成立. 这里所谓的 Hansen 链(Hansen chain)是指有子元素集 H，使得该链的每个元素都用到 H 中小于该元素的最大数作为加数. 上面第二个例子是 Hansen 链，对应的 $H=\{1,2,4,8\}$. Knuth 对 $n=12509$ 给出一个 Hansen 链的例子($H=\{1,2,4,8,16,32,64,128,256,512,1024,1041,2082,4164,8328,8345\}$)：

$$1,2,4,8,16,17,32,64,128,256,512,$$
$$1024,1041,2082,4164,8328,8345,12509,$$

它不是 Brauer 链(32 没用到 17)，且对 $n=12509$ 没有这么短的 Brauer 链存在.

有非 Hansen 数吗?

显然 $l(2n) \leqslant l(n)+1$. 可能是 Knuth 用 $l(382)=l(191)=11$ 指出了有严格不等式成立. Thurber 给出使 $l(2n)=l(n)$ 成立的最小偶数是 13818，他还注意到有一对相邻的奇数 22453, 22455

满足此式. Andrew Granville 问是否有 n 满足 $l(4n)=l(2n)=l(n)$?

D. J. Newman 考虑一台计算机,它做一次加法要花一分钱,但做乘法无须花费. 则对 n 的加法链最大花费不是 $\log n$ 而是 $(\log n)^{\frac{1}{2}+o(1)}$,这里的 log 以 2 为底.

作为一篇好的综述和问题列表,请看 Subbarao 的文章.

参考文献

Walter Aiello & M. V. Subbarao, A conjecture in addition chains related to Scholz's conjecture, *Math. Comput.*, **61**(1993) 17–23; *MR* **93k**:11015.

A. T. Brauer, On addition chains, *Bull. Amer. Math. Soc.*, **45**(1939) 736–739.

A. Cottrell, A lower bound for the Scholz-Brauer problem, Abstract 73T-A200, *Notices Amer. Math. Soc.*, **20**(1973) A-476.

Paul Erdős, Remarks on number theory III. On addition chains, *Acta Arith.*, **6**(1960) 77–81.

R. P. Giese, PhD thesis, University of Houston, 1972.

R. P. Giese, A sequence of counterexamples of Knuth's modification of Utz's conjecture, Abstract 72T-A257, *Notices Amer. Math. Soc.*, **19**(1972) A-688.

A. A. Gioia & M. V. Subbarao, The Scholz-Brauer problem in addition chains II, *Congr. Numer. XXII*, Proc. 8th Manitoba Conf. Numer. Math. Comput. 1978, 251–274; *MR* **80i**: 10078; *Zbl.* 408.10037.

A. A. Gioia, M. V. Subbarao & M. Sugunamma, The Scholz-Brauer problem in addition chains, *Duke Math. J.*, **29**(1962) 481–487; *MR* **25** #3898.

W. Hansen, Zum Scholz-Brauerschen Problem, *J. reine angew. Math.*, **202** (1959) 129–136; *MR***25** #2027.

Kevin Hebb, Some problems on addition chains, thesis, Univ. of Alberta, 1974.

A. M. Il'in, On additive number chains (Russian), *Problemy Kibernet.*, **13** (1965) 245–248.

H. Kato, On addition chains, PhD dissertation, Univ. Southern California, June 1970.

Donald Knuth, *The Art of Computer Programming*, Vol. 2, Addison-Wesley, Reading MA, 1969, 398–422.

D. J. Newman, Computing when multiplications cost nothing, *Math. Comput.*, **46**(1986) 255–257.

Arnold Scholz, Aufgabe 253, *Jber. Deutsch. Math.-Verein. II*, **47**(1937) 41–42 (supplement).

Rolf Sonntag, Theorie der Addition Sketten, PhD Technische Universität Hannover, 1975.

K. B. Stolarsky, A lower bound for the Scholz-Brauer problem, *Canad. J. Math.*, **21**(1969) 675–683; *MR* **40** #114.

M. V. Subbarao, Addition chains – some results and problems, in R. A. Mollin

(ed.) Number Theory and Applications, NATO ASI Series, Kluwer, Boston, 1989, pp. 555–574; *MR* **93a**:11105.
E. G. Straus, Addition chains of vectors, *Amer. Math. Monthly*, **71**(1964) 806–808.
E. G. Thurber, The Scholz-Brauer problem on addition chains, *Pacific J. Math.*, **49**(1973) 229–242; *MR* **49** #7233.
E. G. Thurber, On addition chains $l(mn) \le l(n) - b$ and lower bounds for $c(r)$, *Duke Math. J.*, **40**(1973) 907–913.
E. G. Thurber, Addition chains and solutions of $l(2n) = l(n)$ and $l(2^n - 1) = n + l(n) - 1$, *Discrete Math.*, **16**(1976) 279–289; *MR* **55** #5570; *Zbl.* **346**.10032.
W. R. Utz, A note on the Scholz-Brauer problem in addition chains, *Proc. Amer. Math. Soc.*, **4**(1953) 462–463; *MR* **14**, 949.
C. T. Wyburn, A note on addition chains, *Proc. Amer. Math. Soc.*, **16**(1965) 1134.

C7. 钱币兑换问题

给定 $n \geqslant 2$ 个整数 $0 < a_1 < a_2 < \cdots < a_n$，$(a_1, a_2, \cdots, a_n) = 1$，那么，如果 N 足够大，则 $N = \sum_{i=1}^{n} a_i x_i$ 有非负整数解 x_i. 熟知的 Frobenius 的硬币问题(coin problem)是决定使该方程无解的最大的 $N = g(a_1, a_2, \cdots, a_n)$. Sylvester 证明了 $g(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1$，且不可表示成该形状的数的个数是 $(a_1 - 1)(a_2 - 1)/2$. $n = 3$ 的情形首先由 Selmer 和 Beyer 用连分数算法给出了显式解. 他们的结果由 Rödseth，其后又由 Greenberg 作了简化. 对 $n \geqslant 4$ 没有一般的公式. 如果诸 a_i 在算术级数中，Roberts 找到了 g 的值.

人们也寻找 g 的上界. 1942 年 Brauer 证明了

$$g(a_1, a_2, \cdots, a_n) \leqslant \sum_{i=1}^{n} a_i (d_{i-1}/d_i - 1),$$

这里 $d_i = (a_1, a_2, \cdots, a_i)$. Erdös 和 Graham 证明了

$$g(a_1, a_2, \cdots, a_n) \leqslant 2a_{n-1} \lfloor a_n / n \rfloor - a_n$$

(如果 $n = 2$ 且 a_2 为奇数，这是最好可能的结果). 他们定义

$$\gamma(n, t) = \max_{\{a_i\}} g(a_1, a_2, \cdots, a_n),$$

其中最大值取过所有满足$(a_1,a_2,\cdots,a_n)=1$的数$0<a_1<a_2<\cdots<a_n\leqslant t$. 他们的定理表明有$\gamma(n,t)<2t^2/n$,且他们证明了$\gamma(n,t)\geqslant t^2/(n-1)-5t$. Lewin证明了$\gamma(3,t)=\lfloor(t-2)^2/2\rfloor-1$,且一般地对$n\geqslant 3$有

$$g(a_1,a_2,\cdots,a_n)\leqslant\lfloor(a_{n-1}-1)(a_n-2)/2\rfloor-1.$$

Ernst Selmer对我重写C7和C12两节给了许多帮助,下面引用的他的论文包含了直到1976年为止的所有有关文献.

参考文献

E. R. Berlekamp, J. H. Conway & R. K. Guy, *Winning Ways for your Mathematical Plays*, Academic Press, London, 1982, Chap. 18.

Alfred Brauer, On a problem of partitions, *Amer. J. Math.*, **64**(1942) 299–312.

F. Curtis, On formulas for the Frobenius number of a numerical semigroup, *Math. Scand.*, **67**(1990) 190–192.

J. Dixmier, Proof of a conjecture of Erdős and Graham concerning the problem of Frobenius, *J. Number Theory*, **34**(1990) 198–209; *MR* **91g**:11007.

P. Erdős & R. L. Graham, On a linear diophantine problem of Frobenius, *Acta Arith.*, **21**(1972) 399–408.

Harold Greenberg, Solution to a linear diophantine equation for nonnegative integers, *J. Algorithms*, **9**(1988) 343–353; *MR* **89j**:11122.

Mordechai Lewin, On a linear diophantine problem, *Bull. London Math. Soc.*, **5**(1973) 75–78; *MR* **47** #3311.

Niu Xue-Feng, A formula for the largest integer which cannot be represented as $\sum_{i=1}^{s} a_i x_i$, *Heilongjiang Daxue Ziran Kexue Xuebao*, **9**(1992) 28–32; *MR* **93k**:11019.

J. B. Roberts, Note on linear forms, *Proc. Amer. Math. Soc.*, **7**(1956) 465–469.

Ø. J. Rødseth, On a linear Diophantine problem of Frobenius, *J. reine angew. Math.*, **301**(1978) 171–178; *MR* **58** #27741.

Ernst S. Selmer, On the linear diophantine problem of Frobenius, *J. reine angew. Math.*, **293/294**(1977) 1–17; *MR* **56** #246.

E. S. Selmer & Ö. Beyer, On the linear diophantine problem of Frobenius in three variables, *J. reine angew. Math.*, **301**(1978) 161–170.

J. J. Sylvester, *Math. Quest. Educ. Times*, **41**(1884) 21.

Herbert S. Wilf, A circle of lights algorithm for the "money changing problem", *Amer. Math. Monthly*, **85**(1978) 562–565.

C8. 有不同子集和的集合

基数为 $k+1$ 的整数集合 $\{2^i:0\leqslant i\leqslant k\}$ 的所有 2^{k+1} 个子集的和都不相同. Erdös 要求正整数 $a_1<a_2<\cdots<a_m\leqslant 2^k$ 的最大个数 m,使其所有子集和都不相同. 他和 Leo Moser 证明了 $k+1\leqslant m<k+\frac{1}{2}\log k+2$,这里的对数以 2 为底. Noam Elkies 把右边的常数 2 改进为 $\frac{1}{2}\log\pi<0.826$.

Conway 和 Guy 给出一个序列 $u_0=0, u_1=1, u_{n+1}=2u_n-u_{n-r}(n\geqslant 1)$,其中 r 是离 $\sqrt{2n}$ 最近的整数,从它可以导出 $k+2$ 个整数的集合

$$A=\{a_i=u_{k+2}-u_{k+2-i}:1\leqslant i\leqslant k+2\}.$$

他们猜想这个集合的子集和均不相同(对 $k\leqslant 40$ 由 Mike Guy 证明,对 $n\leqslant 79$ 由 Fred Lunnon 证明). 对 $k\geqslant 21$ 有 $u_{k+2}<2^k$,从而对 $k\geqslant 21$ 有 $m\geqslant k+2$,因为只要找到一个具有想要的基数的集合,通过把每一个数的大小加倍,并添上数 1(或添上任何奇数),就可以增加它的基数了. Conway 和 Guy 猜想,本质上 A 给出该问题的最好可能的解 $m=k+2$,尽管 Lunnon 定义了一类推广的 Conway-Guy 序列,这些序列中有一些给出了比 $u_n/2^n$ (≈ 0.23512531)更小的极限(例如 0.220963). Erdös 悬赏 500 美元给证明或推翻 $m=k+O(1)$ 者.

参考文献

J. H. Conway & R. K. Guy, Sets of natural numbers with distinct sums, *Notices Amer. Math. Soc.*, **15**(1968) 345.

J. H. Conway & R. K. Guy, Solution of a problem of P. Erdős, *Colloq. Math.*, **20**(1969) 307.

P. Erdős, Problems and results in additive number theory, *Colloq. Théorie des Nombres, Bruxelles*, 1955, Liège & Paris, 1956, 127–137, esp. p. 137.

Noam Elkies, An improved lower bound on the greatest element of a sum-

distinct set of fixed order, *J. Combin. Theory Ser. A*, **41**(1986) 89–94; *MR* **87b**:05012.

Martin Gardner, Number 5, *Science Fiction Puzzle Tales*, Penguin, 1981.

Hansraj Gupta, Some sequences with distinct sums, *Indian J. Pure Math.*, **5**(1974) 1093–1109; *MR* **57** #12440.

Richard K. Guy, Sets of integers whose subsets have distinct sums, *Ann. Discrete Math.* **12**(1982) 141–154.

B. Lindström, On a combinatorial problem in number theory, *Canad. Math. Bull.*, **8**(1965) 477–490.

B. Lindström, Om et problem av Erdős for talfoljder, *Nordisk. Mat. Tidskrift*, **161**-2(1968) 29–30, 80.

W. Fred Lunnon, Integer sets with distinct subset-sums, *Math. Comput.*, **50**(1988) 297–320.

Paul Smith, Problem E 2536*, *Amer. Math. Monthly*, **82**(1975) 300. Solutions and comments, **83**(1976) 484.

C9. 用元素对之和作填充

设 m 是在一个 **Sidon 序列**(Sidon sequence)中整数 $1 \leqslant a_1 < a_2 < \cdots < a_m \leqslant n$ 的最大个数,所谓 Sidon 序列,就是其中所有数对之和 $a_i + a_j$ 均不相同. 已知有

$$n^{1/2}(1-\varepsilon) < m \leqslant n^{1/2} + n^{1/4} + 1.$$

这里的上界属于 Lindström,他改进了 Erdös 和 Turán 的一个结果. 而下界属于 Singer. Erdös 和 Turán 问是否有 $m = n^{1/2} + O(1)$?Erdös 悬赏 500 美元给解决此问题者.

Cameron 和 Erdös 要求其元素至多是 n 的 Sidon 序列的个数 $F(n)$. 设 m 如上定义,则我们甚至还不知道是否有 $F(n)/2^m \to \infty$,我们仅仅知道其上极限是无限的. Cameron 和 Erdös 相信有 $F(n) < n^{\varepsilon\sqrt{n}}$. 他们也希望能给出极大 Sidon 序列(即不能再有 $a \leqslant n$ 添加进去的 Sidon 序列)个数的估计.

如果 $\{a_i\}$ 继续代表一无穷序列, Erdös 和 Turán 证明了 $\limsup a_k/k^2 = \infty$,并给出了一个满足 $\liminf a_k/k^2 < \infty$ 的序列. Ajtai, Komlós 和 Szemerédi 证明了存在满足 $a_k < ck^3/\ln n$ 的序列.

Erdös 和 Rényi 证明了:存在一个满足 $a_k < k^{2+\varepsilon}$ 的序列,对此序列,$a_i + a_j = t$ 的解数 $\leqslant c$.

Erdös 注意到有 $\sum_{i=1}^{x} a_i^{-1/2} < c(\ln x)^{1/2}$,并且问这是否是最好可能的结果?他问:当 $x\to\infty$时

$$\frac{1}{\ln x}\sum_{a_i+a_j\leqslant x}\frac{1}{a_i+a_j}\to 0$$

是否为真?他认为似有

$$\sum_{a_i+a_j<x}\frac{1}{a_i+a_j}<c_1\ln\ln x.$$

已知它能$>c_2\ln\ln x$.

Erdös 还问:是否一个 Sidon 序列 $a_1<a_2<\cdots<a_k$ 可以被加长成一个完全差集(见 C10),即

$$a_1<a_2<\cdots<a_k<a_{k+1}<\cdots<a_{p+1}=p^2+p+1,$$

使得诸差 $a_u-a_v(1\leqslant u,v\leqslant p+1,u\neq v)$表示 mod p^2+p+1 的每个非零剩余类恰好一次?

他甚至无法确定它是否能被加长成

$$a_1<a_2<\cdots<a_k<a_{k+1}<\cdots<a_n,a_n<(1+o(1))n^2,$$

即,是否能把它变得渐近地尽可能的稠密?

设 $a_1<a_2<\cdots<a_n$ 为任一整数序列. 下述结论是否为真:它包含一个满足 $m=(1+o(1))n^{\frac{1}{2}}$的 Sidon 子序列 $a_{i_1},\cdots,a_{i_m}$吗?Komlós,Sulyok 和 Szemerédi(见 E11)对 $m>cn^{\frac{1}{2}}$证明了此结论.

如果 $f(n)$是 $n=a_i+a_j$ 的解数,是否有一个满足

$$\lim f(n)/\ln n=c$$

的序列存在? Erdös 和 Turán 猜想:如果对所有充分大的 n 有 $f(n)>0$,或者对所有 k 有 $a_k<ck^2$,那么 $\limsup f(n)=\infty$. Erdös 还悬赏 500 美元给解决此问题者.

Graham 和 Sloane 将此问题重新表述成两种更为明显的填充形式:

令 $v_\alpha(k)(v_\beta(k))$表示存在一个有下述性质的 k-元素的整数集$A=\{0=a_1<a_2<\cdots<a_k\}$的最小的 v:对 $i<j(i\leqslant j)$诸和

$a_i + a_j$ 均属于$[0, v]$且表示$[0, v]$中的每一个元素至多一次. 与 v_β 相伴的集合 A 常称为$\boldsymbol{B_2}$**-序列**(B_2-sequence)(与 E28 比较).

他们给出了 v_α 和 v_β 的值,这些值放在表 3 中. 他们还注意到,对 Erdös-Turán 的方法加以修改可得到界

$$2k^2 - O(k^{3/2}) < v_\alpha, v_\beta < 2k^2 + O(k^{36/23}).$$

表 3 v_α与v_β 的值和集合之范例

k	$v_\alpha(k)$	A 的例子	$v_\beta(k)$	A 的例子
2	1	{0,1}	2	{0,1}
3	3	{0,1,2}	6	{0,1,3}
4	6	{0,1,2,4}	12	{0,1,4,6}
5	11	{0,1,2,4,7}	22	{0,1,4,9,11}
6	19	{0,1,2,4,7,12}	34	{0,1,4,10,12,17}
7	31	{0,1,2,4,8,13,18}	50	{0,1,4,10,18,23,25}
8	43	{0,1,2,4,8,14,19,24}	68	{0,1,4,9,15,22,32,34}
9	63	{0,1,2,4,8,15,24,29,34}	88	{0,1,5,12,25,27,35,41,44}
10	80	{0,1,2,4,8,15,24,29,34,46}	110	{0,1,6,10,23,26,34,41,53,55}

Cilleruelo 证明了:存在一个序列$\{a_k\}$,$a_k \ll k^2$,使诸和 $a_i^2 + a_j^2$ 皆不相同.

如果 $g(m)$是有下述性质的最大整数:每个有 m 个元素的整数集都包含一个有 n 个元素的子集,该子集两两元素之和均不相同. 则 Abbott 证明了:对任何常数 $c < \frac{2}{25}$和所有充分大的 m 有 $g(m) > cm^{1/2}$.

1956 年,Erdös 证明了:存在序列 S,使所有充分大的整数 n 皆可表为S 的两个元素之和,其表法数在 $c_1 \ln n$ 和$c_2 \ln n$ 之间. 最近 Erdös 和 Tetali 对 S 的k 个元素之和得到了相应的结果.

参考文献

Harvey L. Abbott, Sidon sets, *Canad. Math. Bull.*, **33**(1990) 335–341; *MR* **91k**: 11022.

Miklós Ajtai, János Komlós & Endre Szemerédi, A dense infinite Sidon sequence, *European J. Combin.*, **2**(1981) 1–11; *MR* **83f**:10056.

R. C. Bose & S. Chowla, Theorems in the additive theory of numbers, *Comment. Math. Helv.*, **37**(1962-63) 141–147.

Javier Cilleruelo, B_2-sequences whose terms are squares, *Acta Arith.*, **55** (1990) 261–265; *MR* **91i**:11023.

Javier Cilleruelo & Antonio Córdoba, $B_2[\infty]$-sequences of square numbers, *Acta Arith.*, **61**(1992) 265–270.

P. Erdős, Some of my forgotten problems in number theory, *Hardy-Ramanujan J.*, **15** (1992) 34–50.

P. Erdős & R. Freud, On sums of a Sidon-sequence, *J. Number Theory*, **38**(1991) 196–205.

P. Erdős & R. Freud, On Sidon-sequences and related problems (Hungarian), *Mat. Lapok*, **2**(1991) 1–44.

P. Erdős & W. H. J. Fuchs, On a problem of additive number theory, *J. London Math. Soc.*, **31**(1956) 67–73.

P. Erdős & E. Szemerédi, The number of solutions of $m = \sum_{i=1}^{k} x_i^k$, *Proc. Symp. Pure Math. Amer. Math. Soc.*, **24**(1973) 83–90.

Paul Erdős, Melvyn B. Nathanson & Prasad Tetali, Independence of solution sets and minimal asymptotic bases (preprint, 1993).

Paul Erdős & Prasad Tetali, Representations of integers as the sum of k terms, *Random Structures Algorithms*, **1**(1990) 245–261; *MR* **92c**:11012.

P. Erdős & P. Turán, On a problem of Sidon in additive number theory, and on some related problems, *J. London Math. Soc.*, **16**(1941) 212–215; *MR* **3**, 270. Addendum, **19**(1944) 208; *MR* **7**, 242.

R. L. Graham & N. J. A. Sloane, On additive bases and harmonious graphs, *SIAM J. Alg. Discrete Math.*, **1**(1980) 382–404.

H. Halberstam & K. F. Roth, *Sequences*, 2nd Edition, Springer, New York, 1982, Chapter 2.

Jia Xing-De, Some problems and results on subsets of asymptotic bases, *Qufu Shifan Daxue Xuebao Ziran Kexue Ban*, **13**(1987) 45–49; *MR* **88k**:11015.

Jia Xing-De, On the distribution of a B_2-sequence, *Qufu Shifan Daxue Xuebao Ziran Kexue Ban*, **14**(1988) 12–18; *MR* **89j**:11023.

Jia Xing-De, On finite Sidon sequences, *J. Number Thoery*, **44**(1993) 84–92.

F. Krückeberg, B_2-Folgen und verwandte Zahlenfolgen, *J. reine angew. Math.*, **206**(1961) 53–60.

B. Lindström, An inequality for B_2-sequences, *J. Combin. Theory*, **6**(1969) 211–212; *MR* **38** #4436.

Imre Z. Ruzsa, A just basis, *Monatsh. Math.*, **109**(1990) 145–151; *MR* **91e**: 11016.

J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43**(1938) 377–385; *Zbl* **19**, 5.

Vera T. Sós, An additive problem in different structures, *Graph Theory, Combinatorics, Algorithms, and Applications*, (SIAM Conf., San Francisco, 1989), 1991, 486–510; *MR* **92k**:11026.

C10. 模差集和纠错码

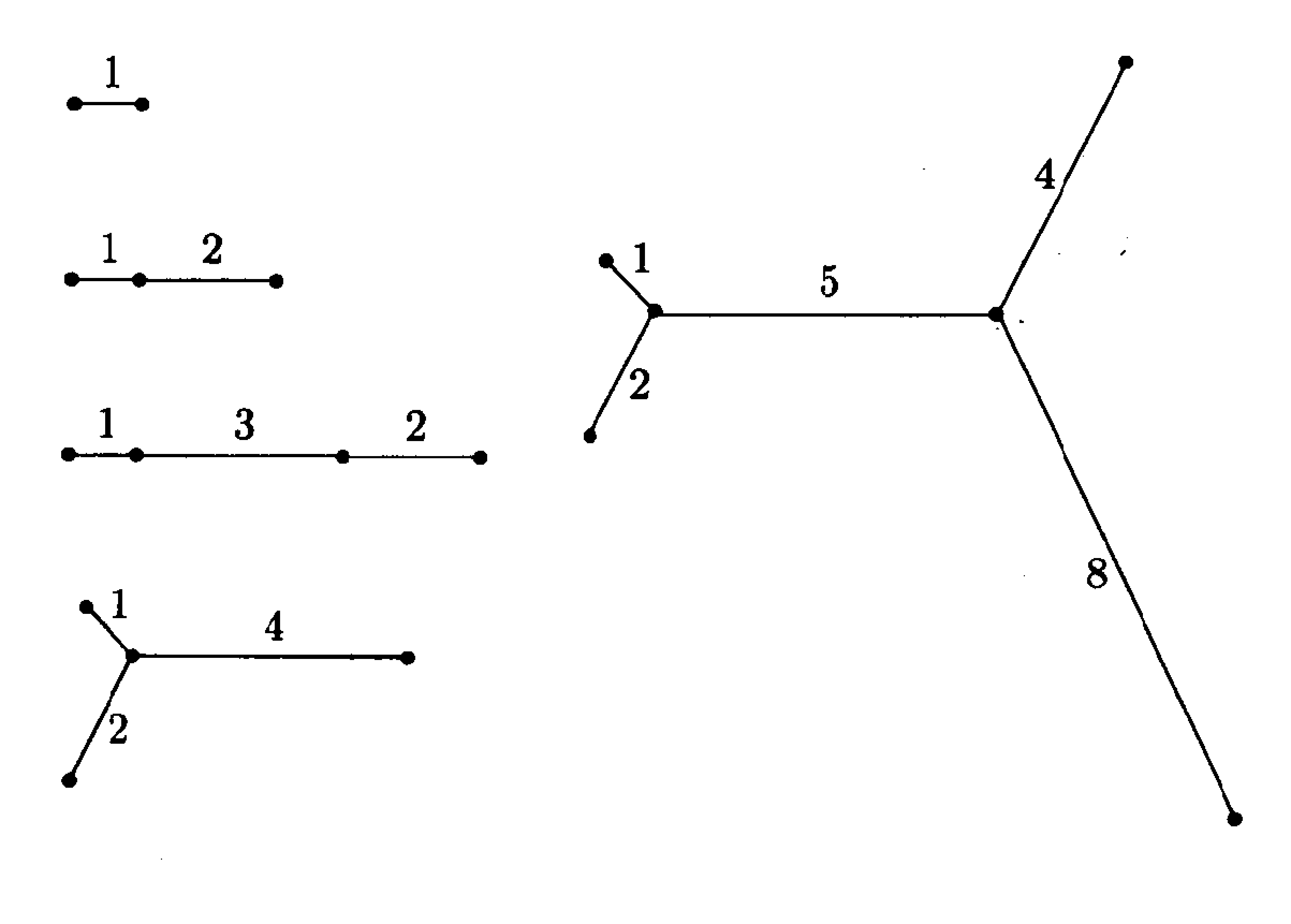
在问题 C9 中提到的 Singer 的结果基于**完全差集**(perfect difference set),所谓完全差集是一个剩余类集 $a_1, a_2, \cdots, a_{k+1} \pmod n$,模 n 的每一个剩余类都可以惟一表成 $a_i - a_j$ 的形式. 例如 $\{1,2,4\} \bmod 7$ 和 $\{1,2,5,7\} \bmod 13$. 仅当 $n = k^2 + k + 1$ 时存在完全差集,Singer 证明了:只要 k 是一个素数幂,这样的集合就存在. Marshall Hall 证明了:非素数幂的数不能用作为 k 的值;Evans和 Mann 证明了在 $k < 1600$ 中不存在非素数幂者. 人们猜想:除非 k 是素数幂,否则无完全差集存在.

如果一个给定的有限序列不包含重复的差,它能否被扩大成为一个完全差集呢?

完全差集可以用来做 **Golomb 尺**(Golomb ruler). 从差集的元素中减去 1,例如 $\{0,1,4,6\}$,并在一根长为 6 的尺上取该集合中的数作为刻度,这根尺可以用来测量所有长度 1,2,3,4,5,6. 更为一般地,我们可以来寻找长为 n、有 $k+1$ 个刻度 $\{0, a_1, \cdots, a_{k-1}, n\}$ 且满足各种不同条件的不完全尺. 例如,(a)所有 $\binom{k+1}{2}$ 个距离都不相等;(b)对给定的 n 和 k 有最大个数的不同距离;(c)从 1 直到某个最大值 e 的所有整数距离都是可用此尺测量的. 对 $k \geqslant 4$ 我们不能满足所有这些条件,但 Leech 发现了完全"连结的"尺的例子. 下列的树

有所指出长度的边,可能被用来测量从 1 直到 1,3,6,6,15 的所有长度.

Gibbs 和 Slater, Herbert Taylor 以及 Yang Yuan-Sheng 把 Leech 有关路径和更一般的树的结果改进为



n	2	3	4	5	6	7	8	9	10	11	12
路径	1	3	6	9	13	18	24	29	37	45	(51)
树	1	3	6	9	15	20	26	34	41	(48)	(55)

这里括号中的数不一定是最好可能的. 它们和图的优美标号及协调标号有联系,见 C13 以及本系列丛书中可能即将出版的组合卷.

Graham 和 Sloane 把差集问题作为 C9 的填充问题的模的形式表达出来. 他们定义 $v_\gamma(k)(v_\delta(k))$为满足下列条件的最小的数 v:存在整数的一个子集 $A=\{0=a_1<a_2<\cdots<a_k\}(\bmod v)$,使得每个 r 可以用至多一种方式写成 $r\equiv a_i+a_j \bmod v$, $i<j$ $(i\leqslant j)$.

他们对 v_γ 的兴趣在于它对纠错码(error-correcting code)的应用. 如果 $A(k,2d,w)$是有 w 个 1、$k-w$ 个零的二元向量(即长度(length)为 k、权(weight)为 w 的词(word))的最大个数,其中任意两个向量至少在 $2d$ 个位置上取不同的值,那么有(对 $d=3$)

$$A(k,6,w)\geqslant\binom{k}{w}\Big/v_\gamma(k)$$

(对一般的 d 的结果要用到有"所有 $d-1$ 个不同元素的和均不相同 mod v"这一性质的集合).

他们注意到 $A(k,2d,w)$ 被 Erdös 和 Hanani，被 Schönheim 研究过，被 Stanton, Kalbfleisch 和 Mullin 在极端集合论中也研究过. 令 $D(t,k,v)$是一个 v-元素集S 的那种k-元素子集的最大个数：S 的每个 t-元素子集都包含在至多一个这样的k-元素子集中. 那么有 $D(t,k,v)=A(v,2k-2t+2,k)$.

表 4 中 v_δ 的值取自 Baumer 的表 6.1，而 v_γ 的值取自 Graham 和 Sloane，他们给出下面的界：

$$k^2-O(k)<v_\gamma(k)<k^2+O(k^{36/23}),$$

$$k^2-k+1\leqslant v_\delta(k)<k^2+O(k^{36/23}).$$

只要 $k-1$ 是一个素数幂，后一式中左边的等号就成立.

表 4 v_γ 与v_δ 的值和集合之范例

k	$v_\gamma(k)$	A 的例子	$v_\delta(k)$	A 的例子
2	2	{0,1}	3	{0,1}
3	3	{0,1,2}	7	{0,1,3}
4	6	{0,1,2,4}	13	{0,1,3,9}
5	11	{0,1,2,4,7}	21	{0,1,4,14,16}
6	19	{0,1,2,4,7,12}	31	{0,1,3,8,12,18}
7	28	{0,1,2,4,8,15,20}	48	{0,1,3,15,20,38,42}
8	40	{0,1,5,7,9,20,23,35}	57	{0,1,3,13,32,36,43,52}
9	56	{0,1,2,4,7,13,24,32,42}	73	{0,1,3,7,15,31,36,54,63}
10	72	{0,1,2,4,7,13,23,31,39,59}	91	{0,1,3,9,27,49,56,61,77,81}

参 考 文 献

L. D. Baumert, *Cyclic Difference Sets*, Springer Lect. Notes Math. **182**, New York, 1971.

M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko & N. J. A. Sloane, Bounds for binary codes of length less than 25, *IEEE Trans. Inform. Theory*, **IT-24**(1978) 81–93.

F. T. Boesch & Li Xiao-Ming, On the length of Golomb's rulers, *Math. Appl.*, **2**(1989) 57–61; *MR* **91h**:11015.

J. H. Conway & N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1988.

P. Erdős & H. Hanani, On a limit theorem in combinatorical analysis, *Publ. Math. Debrecen*, **10**(1963) 10–13.

T. A. Evans & H. Mann, On simple difference sets, *Sankhyā*, **11**(1951) 357–364; *MR* **13**, 899.

Richard A. Gibbs & Peter J. Slater, Distinct distance sets in a graph, *Discrete Math.*, **93**(1991) 155–165.

M. J. E. Golay, Note on the representation of 1, 2, ..., n by differences, *J. London Math. Soc.*(2), **4**(1972) 729–734; *MR* **45** #6784.

R. L. Graham & N. J. A. Sloane, Lower bounds for constant weight codes, *IEEE Trans. Inform. Theory*, **IT-26**(1980) 37–43; *MR* **81d**:94026.

R. L. Graham & N. J. A. Sloane, On additive bases and harmonious graphs, *SIAM J. Algebraic Discrete Methods*, 1(1982) 382–404; *MR* **82f**:10067.

M. Hall, Cyclic projective planes, *Duke Math. J.*, **14**(1947) 1079–1090; *MR* **9**, 370.

John Leech, On the representation of 1, 2, ..., n by differences, *J. London Math. Soc.*, **31**(1956) 160–169; *MR* **19**, 942f.

John Leech, Another tree labelling problem, *Amer. Math. Monthly*, **82**(1975) 923–925.

F. J. MacWilliams & N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

J. C. P. Miller, Difference bases: three problems in the additive theory of numbers, A. O. L. Atkin & B. J. Birch (editors) *Computers in Number Theory*, Academic Press, London, 1971, pp. 299–322; *MR* **47** #4817.

J. Schönheim, On maximal systems of k-tuples, *Stud. Sci. Math. Hungar.*, **1**(1966) 363–368.

R. G. Stanton, J. G. Kalbfleisch & R. C. Mullin, Covering and packing designs, *Proc. 2nd Conf. Combin. Math. Appl.*, Chapel Hill, 1970, 428–450.

Herbert Taylor, A distinct distance set of 9 nodes in a tree of diameter 36, *Discrete Math.*, **93**(1991) 167–168.

B. Wichmann, A note on restricted difference bases, *J. London Math. Soc.*, **38**(1963) 465–466; *MR* **28** #2080.

C11. 有不同和的三-子集

我们可以推广 C9 和 E28 的思想，定义 **B_h-序列**(B_h-sequence)是其中所有 h 个项的和均不相同的序列. Bose 和 Chowla 证明了，如果 $A_h(n)$是$[1,n]$中 B_h-序列的最大基数，那么

$$A_h(n) \geqslant n^{1/h}(1+o(1)).$$

在相反的方向上，贾兴德(Jia Xing-De)证明了，如果 $h=2k$，则有

$$A_h(n) \leqslant k^{1/2k}(k!)^{1/k}n^{1/h}(1+o(1)).$$

对 $h=2k-1$，Chen Sheng 和 Graham 相互独立地证明了界

$$A_h(n) \leqslant (k!)^{2/(2k-1)}n^{1/h}(1+o(1)).$$

对 $h=3$，Graham 得到进一步小小的改进

$$A_3(n) \leqslant \left(4-\frac{1}{228}\right)^{\frac{1}{3}}n^{\frac{1}{3}}(1+o(1)).$$

在无穷的情形，Erdös 悬赏 500 美元给证明或推翻结论

$$¿\quad \liminf \frac{A_h(n)}{n^{1/h}} = 0 \quad ?$$

者. 对 $h=2$ 它由 Erdös 本人给出了证明，而对 $h=4$ 则由 Nash 给出了证明. $h=6$ 的情形由贾兴德予以处理，更一般地，Chen Sheng 证明了：如果 $h=2k$ 为偶数，则

$$\liminf A_h(n)\left(\frac{\ln n}{n}\right)^{1/h} < \infty.$$

剩下未解决的问题是当 h 为奇数时证明此结论.

陈文德(Chen Wen-De)和 Kløve 的论文给出有关 B_h-序列的电子工程文献的参考资料.

参考文献

W. C. Babcock, Intermodulation interference in radio systems, *Bell Systems Tech. J.*, **32**(1953) 63–73.

R. C. Bose & S. Chowla, *Report Inst. Theory of Numbers*, Univ. of Colorado, Boulder, 1959, p. 335.

R. C. Bose & S. Chowla, Theorems in the additive theory of numbers, *Comment. Math. Helvet.*, **37**(1962-63) 141–147.

Sheng Chen, On size of finite Sidon sequences, *Proc. Amer. Math. Soc.*, (to appear).

Sheng Chen, A note on B_{2k}-sequences, *J. Number Theory*, (1994)

Sheng Chen, On Sidon sequences of even orders, *Acta Arith.*, **64**(1993) 325–330.

Chen Wen-De & Torliev Kløve, Lower bounds on multiple difference sets, *Discrete Math.*, **98**(1991) 9–21; *MR* 93a:05028.

S. W. Graham, Upper bounds for B_3-sequences, Abstract 882-11-25, *Abstracts Amer. Math. Soc.*, **14**(1993) 416.

S. W. Graham, Upper bounds for Sidon sequences, (preprint 1993).

D. Hajela, Some remarks on $B_h[g]$-sequences, *J. Number Theory*, **29**(1988) 311–323; *MR* **90d**:11022.

M. Helm, On B_{2k}-sequences, *Acta Arith.*, **63**(1993) 367–371.
M. Helm, A remark on B_{2k}-sequences, *J. Number Theory*, (to appear).
Jia Xing-De, On B_6-sequences, *Qufu Shifan Daxue Xuebao Ziran Kexue Ban*, **15**(1989) 7–11; *MR* **90**j:11022.
Jia Xing-De, on B_{2k}-sequences, *J. Number Theory*, (to appear).
T. Kløve, Constructions of $B_h[g]$-sequences, *Acta Arith.*, **58**(1991) 65–78; *MR* **92**f:11033.
Li An-Ping, On B_3-sequences, *Acta Math. Sinica*, **34**(1991) 67–71; *MR* **92f**: 11037.
B. Lindström, A remark on B_4-sequences, *J. Combin. Theory*, **7**(1969) 276–277.
John C. M. Nash, On B_4-sequences, *Canad. Math. Bull.*, **32**(1989) 446–449; *MR* **91e**: 11025.

C12. 邮票问题

与填充问题 C9 对偶的覆盖问题至少可以追溯到 Rohrbach. 它的一个通俗的形式涉及一组打算用到信封上的整数面值的邮票 $A_k=\{a_1,a_2,\cdots,a_k\}(1=a_1<a_2<\cdots<a_k)$的设计,信封上总共可贴得下至多 h 张邮票,要使得直到一个给定界限为止的所有整数面值的邮票都可以粘贴到信封上. 不能用线性组合 $\sum_{i=1}^{k}x_ia_i\left(x_i\geqslant 0,\sum_{i=1}^{k}x_i\leqslant h\right)$表示的最小的整数 $N(h,A_k)$ 是什么?称连续可取到的邮票面值的个数 $n(h,A_k)=N(h,A_k)-1$ 为 A_k 的 h- 值域(h-range)(德语是 h-Reichweite). A_k 则称为 h 阶加性基(additive basis of order h)或称为 h- 基(h-basis). 一开始主要的兴趣在于“整体的”问题:给定 h 和 k,求具有最大可能的 h- 值域 $n(h,k)=n(h,A_k^*)=\max\limits_{A_k}n(h,A_k)$ 的一个极值基(extremal basis)A_k^*. 最近“局部的”问题也引起了人们的关注:当 h 和一个特别的基 A_k 给定后,试求 $n(h,A_k)$.

局部问题仅当 $k=2$ 和 $k=3$ 得到了完全的解决. 平凡地,对 $h\geqslant a_2-2$ 有 $n(h,A_2)=(h+3-a_2)a_2-2$. Rødseth 发展出一种基于连分数算法的方法,用来确定 $n(h,A_3)$. 由此,Selmer 对大约 99% 的 A_3(渐近地说)导出了显式公式.

Stöhr 从关于 $n(h,A_2)$的公式推出有

$$n(h,2)=\lfloor(h^2+6h+1)/4\rfloor.$$

$k=3$ 的整体问题是由 Hofmeister 解决的，特别地他证明了对 $h\geqslant 20$ 有

$$n(h,3)=\frac{4}{3}\left(\frac{h}{3}\right)^3+6\left(\frac{h}{3}\right)^2+Ah+B,$$

其中 A 和 B 依赖于 h 模 9 的剩余. Mossige 证明了

$$n(h,4)\geqslant 2.008\left(\frac{h}{4}\right)^4+O(h^3),$$

他还和 Kirfel 一起证明了(迄今未发表)：这个界是最好可能的. Kirfel 还证明了：对所有 $k\geqslant 1$ 极限

$$c_k=\lim_{h\to\infty}\frac{n(h,k)}{(h/k)^k}$$

存在. Kolsdorf 证明了

$$n(h,5)\geqslant 3.06\left(\frac{h}{5}\right)^5+O(h^4).$$

Mrose 证明了：对所有正整数 $h-1,h_2,k_1,k_2$ 有

$$n(h_1+h_2,k_1+k_2)\geqslant(n(h_1,k_1)+1)\cdot(n(h_2,k_2)+1) \qquad (*),$$

他还推出，如果 $k_i(i=1,2)$是固定的且

$$n(h,k_i)\geqslant\alpha_i\left(\frac{h}{k_i}\right)^{k_i}+O(h^{k_i-1}),$$

那么

$$n(h,k_1+k_2)\geqslant\alpha_1\alpha_2\left(\frac{h}{k_1+k}\right)^{k_1+k_2}+O(h^{k_1+k_2-1}).$$

于是，如果 x_i 是固定的非负整数，且满足 $k=\sum_{i=1}^{5}ix_i$，那么

$$n(h,k)\geqslant(3.06)^{x_5}(2.008)^{x_4}\left(\frac{4}{3}\right)^{x_3}\left(\frac{h}{k}\right)^k+O(h^{k-1}).$$

对固定的 k，最好的一般性的上界属于 Rødseth:

$$n(h,k)\leqslant\frac{(k-1)^{k-2}}{(k-2)!}\left(\frac{h}{k}\right)^k+O(h^{k-1}).$$

对固定的 h，重点放在 $h=2$ 上. 1937 年 Rohrbach 证明了对

$c_1=1$ 和 $c_2=1.9968$ 有

$$c_1\left(\frac{k}{2}\right)^2+O(k)\leqslant n(2,k)\leqslant c_2\left(\frac{k}{2}\right)^2+O(k).$$

经若干改进之后，最好的已知结果是 $c_1=\frac{8}{7}$（Mrose）和 $c_2=1.9208$（Klotz）. Windecker 证明了

$$n(3,k)\geqslant\frac{4}{3}\left(\frac{k}{3}\right)^3+\frac{16}{3}\left(\frac{k}{3}\right)^2+O(k).$$

再由（$*$），如果 y_i 是满足 $h=\sum_{i=1}^{3}iy_i$ 的固定的非负整数，那么

$$n(h,k)\geqslant\left(\frac{4}{3}\right)^{y_3}\left(\frac{8}{7}\right)^{y_2}\left(\frac{k}{h}\right)^h+O(k^{h-1}).$$

Graham 和 Sloane（与 C9，C10 比较）定义 $n_{\alpha(k)}(n_{\beta(k)})$ 为满足下列条件的最大的数 n：存在 k 个元素的整数集 $A=\{0=a_1<a_2<\cdots<a_k\}$，使 $[1,n]$ 中每个 r 都可以用至少一种方式写成 $r=a_i+a_j$，$i<j(i\leqslant j)$，从而他们的 $n_{\beta(k)}$ 就是这里的 $n(2,k-1)$，而他们的 $n_{\alpha(k)}$ 对应于两张不同面值（包含有一张面值为零的情形）的邮票问题.

在表 5 中他们给出了 $n_{\alpha(k)}$ 和 $n_{\beta(k)}$ 的值.

表 5　$n_\alpha(k)$ 和 $n_\beta(k)$ 的值以及集合之范例

k	$n_{\alpha(k)}$	A 的例子	$n_{\beta(k)}$	A 的例子
2	1	{0,1}	2	{0,1}
3	3	{0,1,2}	4	{0,1,2}
4	6	{0,1,2,4}	8	{0,1,3,4}
5	9	{0,1,2,3,6}	12	{0,1,3,5,6}
6	13	{0,1,2,3,6,10}	16	{0,1,3,5,7,8}
7	17	{0,1,2,3,4,8,13}	20	{0,1,2,5,8,9,10}
8	22	{0,1,2,3,4,8,13,18}	26	{0,1,2,5,8,11,12,13}
9	27	{0,1,2,3,4,5,10,16,22}	32	{0,1,2,5,8,11,14,15,16}
10	33	{0,1,2,3,4,5,10,16,22,28}	40	{0,1,3,4,9,11,16,17,19,20}
11	40	{0,1,2,4,5,6,10,13,20,27,34}	46	{0,1,2,3,7,11,15,19,21,22,24}
12	47	{0,1,2,3,6,10,14,18,21,22,23,24}	54	{0,1,2,3,7,11,15,19,23,25,26,28}
13	56	{0,1,2,4,6,7,12,14,17,21,30,39,48}	64	{0,1,3,4,9,11,16,21,23,28,29,31,32}
14	65	{0,1,2,4,6,7,12,14,17,21,30,39,48,57}	72	{0,1,3,4,9,11,16,20,25,27,32,33,35,36}

$n(h,k)$的更一般的表由 Lunnon 作了计算，而由 Mossige(最近由 Challis)做了扩充.

对这些问题真有兴趣的学生可参考 Selmer 的三卷本的百科全书，它包含有 121 篇文献. 而 Djawadi 和 Hofmeister 有一篇有用的总述，它附有 47 篇文献.

参 考 文 献

M. F. Challis, Two new techniques for computing extremal h-bases A_k, *Comput. J.*, **36**(1993) 117–126. [An updating of the appendix is available from the author.]

Mehdi Djawadi & Gerd Hofmeister, The postage stamp problem *Mainzer Seminarberichte, Additive Zahlentheorie*, **3**(1993) 187–195.

Paul Erdős & Melvyn B. Nathanson, Additive bases with many representations, *Acta Arith.*, **52**(1989) 399–406; *MR* **91e**:11015.

N. Hämmerer & G. Hofmeister, Zu einer Vermutung von Rohrbach, *J. reine angew. Math.*, **286/287**(1976) 239–247; *MR* **54** #10181.

G. Hofmeister, Asymptotische Abschätzungen für dreielementige extremalbasen in natürlichen Zahlen, *J. reine angew. Math.*, **232**(1968) 77–101; *MR* **38** #1068.

G. Hofmeister, Die dreielementigen Extremalbasen, *J. reine angew. Math.*, **339** (1983) 207–214.

G. Hofmeister, C. Kirfel & H. Kolsdorf, Extremale Reichweitenbasen, No. **60**, Dept. Pure Math., Univ. Bergen, 1991.

Jia Xing-De, On a combinatorial problem of Erdős and Nathanson, *Chinese Ann. Math. Ser. A*, 9(1988) 555–560; *MR* **90i**:11018.

Jia Xing-De, On the order of subsets of asymptotic bases, *J. Number Theory* **37**(1991) 37–46; *MR* **92d**:11006.

Jia Xing-De & Melvyn B. Nathanson, A simple construction of minimal asymptotic bases, *Acta Arith.*, **52**(1989) 95–101; *MR* **90g**:11020.

Christoph Kirfel, Extremale asymptotische Reichweitenbasen, *Acta Arith.*, **60** (1992) 279–288; *MR* **92m**:11012.

W. Klotz, Extremalbasen mit fester Elementeanzahl, *J. reine angew. Math.*, **237**(1969) 194–220.

W. Klotz, Eine obere Schranke für die Reichweite einer Extremalbasis zweiter Ordnung, *J. reine angew. Math.*, **238**(1969) 161–168 (and see 194–220); *MR* **40** #117, 116.

W. F. Lunnon, A postage stamp problem, *Comput. J.*, **12**(1969) 377–380; *MR* **40** #6745.

L. Moser, On the representation of 1, 2, ..., n by sums, *Acta Arith.*, **6**(1960) 11–13; *MR* **23** #A133.

L. Moser, J. R. Pounder & J. Riddell, On the cardinality of h-bases for n, *J. London Math. Soc.*, **44**(1969) 397–407; *MR* **39** #162.

S. Mossige, Algorithms for computing the h-range of the postage stamp problem, *Math. Comput.*, **36**(1981) 575–582; *MR* **82e**:10095.

S. Mossige, On extremal h-bases A_4, *Math. Scand.*, **61**(1987) 5–16; *MR* **89e**:11008.

A. Mrose, Untere Schranken für die Reichweiten von Extremalbasen fester Ordnung, *Abh. Math. Sem. Univ. Hamburg*, **48**(1979) 118–124; *MR* **80g**:10058.

Melvyn B. Nathanson, Extremal properties for bases in additive number theory, Number Theory, Vol. I (Budapest, 1987), *Colloq. Math. Soc. János Bolyai* **51**(1990) 437–446; *MR* **91h**:11009.

J. Riddell & C. Chan, Some extremal 2-bases, *Math. Comput.*, **32**(1978) 630–634; *MR* **57** #16244.

Ø. Rødseth, On h-bases for n, *Math. Scand.*, **48**(1981) 165–183; *MR* **82m**: 10034.

Øystein J. Rødseth, An upper bound for the h-range of the postage stamp problem, *Acta Arith.* **54**(1990) 301–306; *MR* **91h**:11013.

H. Rohrbach, Ein Beitrag zur additiven Zahlentheorie, *Math. Z.*, **42**(1937) 1–30; *Zbl.* **15**, 200.

H. Rohrbach, Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretische Frage, *Math. Z.*, **42**(1937) 538–542; *Zbl.* **16**, 156.

Ernst S. Selmer, On the postage stamp problem with three stamp denominations, *Math. Scand.*, **47**(1980) 29–71; *MR* **82d**:10046.

Ernst S. Selmer, The Local Postage Stamp Problem, Part I General Theory, Part II The Bases A_3 and A_4, Part III Supplementary Volume, No. 42, 44, 57, Dept. Pure Math., Univ. Bergen, (86-04-15, 86-09-15, 90-06-12) ISSN 0332-5047. (Available on request.)

Ernst S. Selmer, On Stöhr's recurrent h-bases for N, *Kongel. Norske Vidensk. Selsk.*, Skr. 3, 1986, 15 pp.

Ernst S. Selmer, Associate bases in the postage stamp problem, *J. Number Theory*, **42**(1992) 320–336.

Ernst S. Selmer & Arne Rödne, On the postage stamp problem with three stamp denominations, II, *Math. Scand.*, **53**(1983) 145–156; *MR* **85j**:11075.

Ernst S. Selmer & Björg Kristin Selvik, On Rödseth's h-bases $A_k = \{1, a_2, 2a_2, \ldots, (k-2)a_2, a_k\}$, *Math. Scand.*, **68**(1991) 180–186; *MR* **92k**: 11010.

Alfred Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I, II, *J. reine angew. Math.*, **194**(1955) 40–65, 111–140; *MR* **17**, 713.

R. Windecker, Eine Abschnittsbasis dritter Ordnung, *Kongel. Norske Vidensk. Selsk. Skrifter*, **9**(1976) 1–3.

C13. 对应的模覆盖问题;图的协调标号法

正如 C10 是填充问题 C9 的模的形式一样,我们也可以对覆盖问题 C12 提出相应的模的形式.

Graham 和 Sloane 完成了他们对 $n_\gamma(k)(n_\delta(k))$的 8 个定义

之一,分别定义它们为满足下列条件的最大整数:存在一个模 n 的剩余类的子集 $A=\{0=a_1<a_2<\cdots<a_k\}$,使每个 r 都可以用至少一种方式表示成 $r\equiv a_i+a_j \bmod n, i<j(i\leqslant j)$.

他们称一个有 v 个顶点、$e\geqslant v$ 条边的连通图为**协调的**(harmonious),如果存在图的顶点 x 的一种有不同标号 $l(x)$ 的标号法,使得当边 xy 用 $l(x)+l(y)$ 作标号时,诸条边的标号构成模 e 的一个完全剩余系. 树(对树来说其边数为 $e=v-1$)也称为协调的,如果恰有一个顶点标号被加倍,且边的标号构成模 $v-1$ 的完全剩余系. 它们与本问题的联系在于 $n_\gamma(v)$ 是任意一个有 v 个顶点的协调图的边的最大个数.

例如,从表 6 中我们注意到:$n\gamma(5)=9$ 是由集合 $\{0,1,2,4,7\}$ 得来的,于是在 5 个顶点的协调图中最多可以出现 9 条边(图 6).

表 6　$n_\gamma(k)$、$n_\delta(k)$ 的值和集合之范例

k	$n_\gamma(k)$	A 的例子	$n_\delta(k)$	A 的例子
2	1	—	3	$\{0,1\}$
3	3	$\{0,1,2\}$	5	$\{0,1,2\}$
4	6	$\{0,1,2,4\}$	9	$\{0,1,3,4\}$
5	9	$\{0,1,2,4,7\}$	13	$\{0,1,2,6,9\}$
6	13	$\{0,1,2,3,6,10\}$	19	$\{0,1,3,12,14,15\}$
7	17	$\{0,1,2,3,4,8,13\}$	21	$\{0,1,2,3,4,10,15\}$
8	24	$\{0,1,2,4,8,13,18,22\}$	30	$\{0,1,3,9,11,12,16,26\}$
9	30	$\{0,1,2,4,10,15,17,22,28\}$	35	$\{0,1,2,7,8,11,26,29,30\}$
10	36	$\{0,1,2,3,6,12,19,20,27,33\}$		

Graham 和 Sloane 把协调图和优美图做了比较和对照,我们将在本系列丛书以后要出版的组合卷中来讨论优美图. 一个图是优美的(graceful),如果从 $[0,e]$ 中选取了顶点标号,并利用 $|l(x)-l(y)|$ 计算出边的标号之后,所有边的标号均不相同(即取值 $[1,e]$).

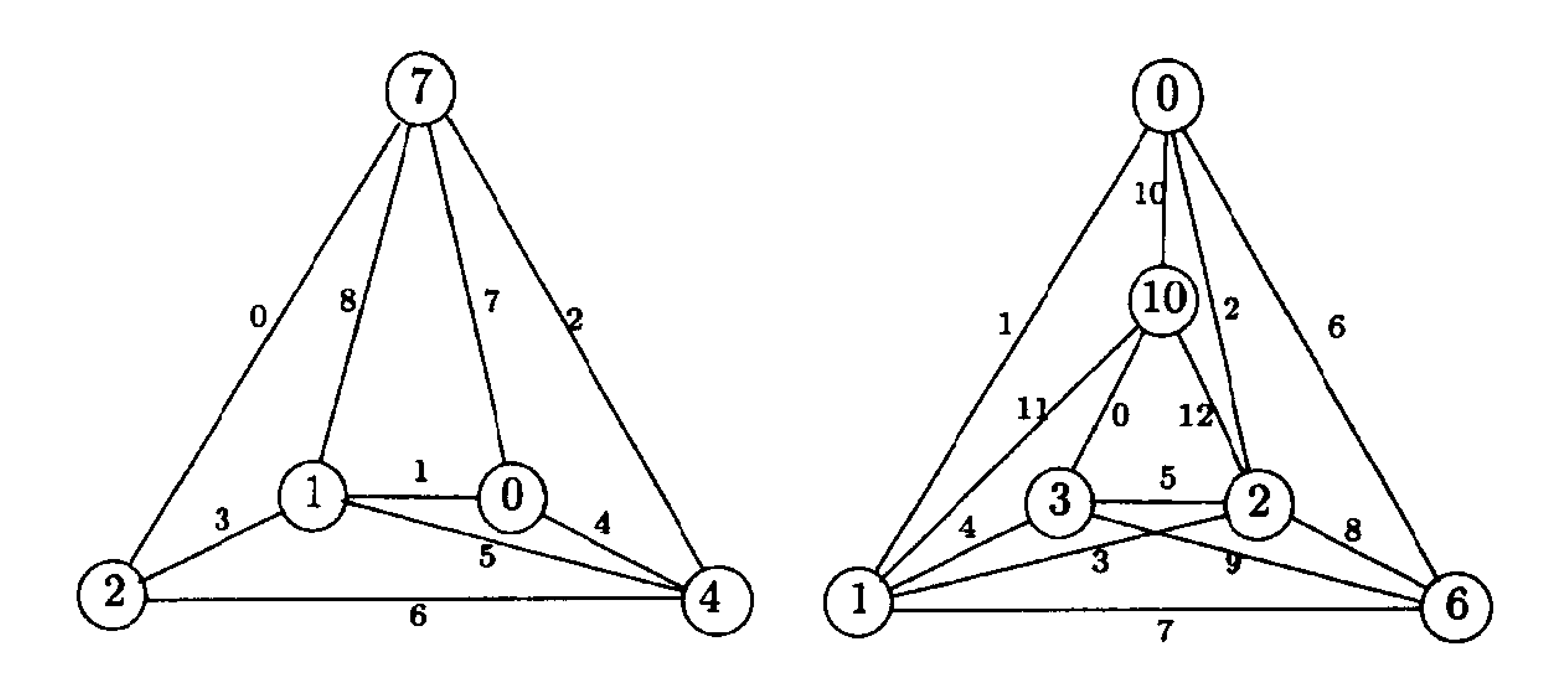


图 6　极大协调图

猜想树既是协调的又是优美的，但这些问题仍未获得解决．一个圈 C_n 恰当 n 为奇数时是协调的，而恰当 $n\equiv 0$ 或 $3 \bmod 4$ 时是优美的．友谊图或风车恰当 $n\not\equiv 2 \bmod 4$ 时是协调的，而恰当 $n\equiv 0$ 或 $1 \bmod 4$ 时是优美的．与 Petersen 图一样，扇图和轮图既是协调的又是优美的．五种柏拉图立体（指正四面体、正六面体、正八面体、正十二面体、正二十面体这五种正多面体——译者注）的图当然都是优美的，人们或许猜想它们也是协调的，但对立方体和正八面体来说并非如此．Joseph Gallian 的文章里有关于图的标号的文献．

参 考 文 献

Joseph A. Gallian, A survey - recent results, conjectures and open problems in labeling graphs, *J. Graph Theory*, **13**(1989) 491-504; *MR* **90k**:05132.

C14．最大无和集

用 $l(n)$ 记满足下列条件的最大整数 l：如果 $a_1, a_2, \cdots, a_n$ 是任何不同的自然数，总可以从中找到 l 个数使得对 $1\leqslant j<k\leqslant l$，$1\leqslant m\leqslant n$ 有 $a_{i_j}+a_{i_k}\neq a_m$．注意 $j\neq k$，否则集合 $\{a_i=2^i \mid 1\leqslant i\leqslant$

$n\}$就蕴含 $l(n)=0$. Klarner 的一个评论表明 $l(n)>c\ln n$. 另一方面,集合$\{2^i+0,\pm1\,|\,1<i\leqslant s+1\}$蕴含 $l(3s)<s+3$,故有 $l(n)<\frac{1}{3}n+3$. Selfridge 利用集合$\{(3m+t)2^{m-i}\,|\,-i<t<i, 1\leqslant i\leqslant m\}$推广了这一结果,他证明了 $l(m^2)<2m$. Choi 利用筛法进一步将此结果改进为 $l(n)\ll n^{0.4+\varepsilon}$.

该问题可以推广成如下问题:对每个 l,是否存在一个 $n_0=n_0(l)$,使得只要 $n>n_0, a_1, a_2, \cdots, a_n$ 是使$a_{i_1}a_{i_2}=e$(单位)不成立的群中任意 n 个元素(这里 i_1, i_2 可以相等,因此没有 1 阶或 2 阶的元素 a_i,也没有其逆也是一个 a_i 的元素a_i),那么就存在 l 个元素 a_i 使得$a_{i_j}\cdot a_{i_k}\neq a_m$, $1\leqslant j<k\leqslant l$, $1\leqslant m\leqslant n$? 即使对 $l=3$,此问题也未获得证明.

对于不包含 $a_1x_1+\cdots+a_kx_k=x_{k+1}$的解的那种集合的推广,见 Funar 和 Moree 的论文.

参考文献

Harvey L. Abbott, On a conjecture of Funar concerning generalized sum-free sets, *Niew Arch. Wisk.*(4), **4**(1991) 249–252.

S. L. G. Choi, On sequences not containing a large sum-free subsequence, *Proc. Amer. Math. Soc.*, **41**(1973) 415–418; *MR* **48** #3910.

S. L. G. Choi, On a combinatorial problem in number theory, *Proc. London Math. Soc.*,(3) **23**(1971) 629–642; *MR* **45** #1867.

P. H. Diananda & Yap H.-P., Maximal sum-free sets of elements of finite groups, *Proc. Japan Acad.*, **45**(1969) 1–5; *MR* **39** #6968.

Louis Funar, Generalized sum-free sets of integers, *Nieuw Arch. Wisk.*(4) **8**(1990) 49–54; *MR* **91e**:11012.

Pieter Moree, On a conjecture of Funar, *Nieuw Arch. Wisk.*(4) **8**(1990) 55–60; *MR* **91e**:11013.

Leo Moser, Advanced problem 4317, *Amer. Math. Monthly*, **55**(1948) 586; solution Robert Steinberg, **57**(1950) 345.

Anne Penfold Street, A maximal sum-free set in A_5, *Utilitas Math.*, **5**(1974) 85–91; *MR* **49** #7156.

Anne Penfold Street, Maximal sum-free sets in abelian groups of order divisible by three, *Bull. Austral. Math. Soc.*, **6**(1972) 317–318; *MR* **47** #5147.

P. Varnavides, On certain sets of positive density, *J. London Math. Soc.*, **34**(1959) 358–360; *MR* **21** #5595.

Edward T. H. Wang, On double-free set of integers, *Ars Combin.*, **28**(1989) 97–100; *MR* **90d**:11011.

Yap Hian-Poh, Maximal sum-free sets in finite abelian groups, *Bull. Austral. Math. Soc.*, **4**(1971) 217–223; *MR* **43** #2081 [and see *ibid*, **5**(1971) 43–54; *MR* **45** #3574; *Nanta Math.*, **2**(1968) 68–71; *MR* **38** #3345; *Canad. J. Math.*, **22**(1970) 1185–1195; *MR* **42** #1897; *J. Number Theory*, **5**(1973) 293–300; *MR* **48** #11356].

C15. 最大无零和集

Erdös 和 Heibronn 要求模 m 的不同剩余类的最大个数 $k = k(m)$，使它不存在和为零的子集．例如集合

$$1, -2, 3, 4, 5, 6$$

表明 $k(20) \geqslant 6$，且事实上等式成立．这个例子的类型表明有

$$k \geqslant \lfloor (-1 + \sqrt{8m+9})/2 \rfloor \qquad (m \geqslant 6),$$

其中等号对 $6 \leqslant m \leqslant 24$ 成立．然而 Selfridge 注意到，如果 m 形如 $2(l^2 + l + 1)$，则集合

$$1, 2, \cdots, l-1, l, \frac{1}{2}m, \frac{1}{2}m + 1, \cdots, \frac{1}{2}m + l$$

蕴含

$$k \geqslant 2l + 1 = \sqrt{2m - 3}.$$

事实上他猜想对任何偶数 m，这个集合或去掉 l 的集合总是给出最好的结果．例如 $k(42) \geqslant 9$.

另一方面，如果 p 是区间

$$\frac{1}{2}k(k+1) < p < \frac{1}{2}(k+1)(k+2)$$

中的一个素数，他猜想有 $k(p) = k$，这里取到此值的集合可以直接取为

$$1, 2, \cdots, k.$$

Clement Lam 证实有 $k(43) = 8$，故而 k 不是 m 的单调函数．

已知有比 $k \geqslant \sqrt{2m-3}$ 更好的不等式的仅有的情形是 $k(25) \geqslant \sqrt{50-1} = 7$，这正如集合 1, 6, 11, 16, 21, 5, 10 所表明的那样．如果 m 形如 $25l(l+1)/2$ 且为奇数，则有可能对集合 1,

$-2,3,4,\cdots$做出改进，但是如果 m 有此形状且为偶数，则对此种偶数 m 给出的结果总是更好一些.

是否对无穷多个 m 的值有 $k=\lfloor(-1+\sqrt{8m+9})/2\rfloor$呢?

对何种 m 的值能得到集合，其元素均不与 m 互素呢? 例如 $m=12$: $\{3,4,6,10\}$或$\{4,6,9,10\}$. 存在 m 的值，使所有得到的集合都是这种类型吗?

Erdös 和 Heibronn 证明了，如果 $a_1,a_2,\cdots,a_k$, $k\geqslant 3(6p)^{1/2}$是模 p 的不同剩余类，p 是素数，那么模 p 的每个剩余类都可以写成 $\sum_{i=1}^{k}\varepsilon_i a_i$ ($\varepsilon=0$ 或 1) 的形式. 他们猜想同样的结论对 $k>2\sqrt{p}$ 也成立，且这是最好可能的结果，Olsen 则对此给出了证明. 他们又进一步猜想：形如 a_i+a_j $(1\leqslant i<j\leqslant k)$的不同剩余类的个数 s 至少是 $\min\{p,2k-3\}$. Mansfield, Rødseth, Freiman, Low 和 Pitman 得到了部分结果. Dias da Silva 和 Hamidoune 对 Erdös-Heibronn 猜想给出了完全的证明，事实上他们证明了：如果 A^h 表示A 的所有h 个不同元素之和组成的集合，$A\subseteq Z/pZ$，$|A|=k$，那么$|A^h|\geqslant\min\{p,hk-h^2+1\}$. Nathanson 简化了他们的证明，且和 Ruzsa 一起证明了：如果 $A,B\subseteq Z/pZ$，$|A|=k>l=|B|$，那么$|\{a+b:a\in A,b\in B,a\neq b\}|\geqslant\min\{p,k+l-2\}$.

参 考 文 献

W. Brakemeier, *Ein Beitrag zur additiven Zahlentheorie*, Dissertation, Tech. Univ. Braunschweig 1973.

W. Brakemeier, Eine Anzahlformel von Zahlen modulo n, *Monatsh. Math.*, **85** (1978) 277–282.

A. L. Cauchy, Recherches sur les nombres, *J. École Polytech.*, **9**(1813) 99–116.

H. Davenport, On the addition of residue classes, *J. London Math. Soc.*, **10**(1935) 30–32.

H. Davenport, A historical note, *J. London Math. Soc.*, **22**(1947) 100–101.

J. A. Dias da Silva & Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.*, (to appear).

P. Erdős, Some problems in number theory, in *Computers in Number Theory*, Academic Press, London & New York, 1971, 405–413.

P. Erdős & H. Heilbronn, On the addition of residue clesses mod p, *Acta Arith.*,

9(1969) 149–159.
G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Transl. Math. Monographs, **37**(1973), Amer. Math. Soc., Providence RI.
G. A. Freiman, L. Low & J. Pitman, 1993 preprint.
Henry B. Mann & John E. Olsen, Sums of sets in the elementary abelian group of type (p, p), *J. Combin. Theory*, **2**(1967) 275–284.
R. Mansfield, How many slopes in a polygon? *Israel J. Math.*, **39**(1981) 265–272; *MR* **84**j:03074.
M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, 1994.
M. B. Nathanson & I. Z. Ruzsa, Sums of different residues modulo a prime, 1993 preprint.
John E. Olsen, An addition theorem modulo p, *J. Combin. Theory*, **5**(1968) 45–52.
John E. Olsen, An addition theorem for the elementary abelian group, *J. Combin. Theory*, **5**(1968) 53–58.
J. M. Pollard, A generalisation of the theorem of Cauchy and Davenport, *J. London Math. Soc.*, **8**(1974) 460–462.
J. M. Pollard, Addition properties of residue classes, *J. London Math. Soc.*, **11**(1975) 147–152.
U.-W. Rickert, *Über eine Vermutung in der additiven Zahlentheorie*, Dissertation, Tech. Univ. Braunschweig 1976.
Øystein J. Rødseth, Sums of distinct residues mod p, *Acta Arith.*, **65**(1993) 181–184.
C. Ryavec, The addition of residue classes modulo n, *Pacific J. Math.*, **26** (1968) 367–373.
E. Szemerédi, On a conjecture of Erdős and Heilbronn, *Acta Arith.*, **17**(1970-71) 227–229.

C16. 非均值集;非整除集

整数 $0 \leqslant a_1 < a_2 < \cdots < a_n \leqslant x$ 的非均值集(nonaveraging set) A 是由 Erdös 和 Straus 根据下述性质定义的:该集合中没有哪个元素 a_i 能是 A 的某个多于一个元素的子集的算术平均. 用 $f(x)$ 表示这样的一个集合中元素的最大个数;$g(x)$表示$[0, x]$中满足下述性质的整数子集 B 中元素的最大个数;B 的任何两个不同子集的算术平均都不相同;用 $h(x)$表示使 B 的子集有不同基数的那种集合B 中元素的最大个数. Erdös 和 Straus 以及 Abbott 证明了(用到 E10 中 Szemerédi 的结果):

$$\frac{1}{10}\log x + O(1) < \log f(x) < \frac{2}{3}\log x + O(1)$$

$$\frac{1}{2}\log x - 1 < g(x) < \log x + O(\ln\ln x)$$

$$\sqrt{\ln x} - 1 + O(1/\sqrt{\ln x}) < \log h(x) < 2\log \ln x + O(1),$$

他们猜想有 $f(x) = \exp(c\sqrt{\ln x}) = o(x^{\varepsilon})$ 和 $h(x) = (1 + o(1))\log x$ ($\log x = (\ln x)/(\ln 2)$ 是以 2 为底的对数). 后来 Abbott 将常数 $\frac{1}{10}$ 改进为 $\frac{1}{5}$, 而 Bosznay 则将它改进为 $\frac{1}{4}$, Erdös 和 Sárközy 则将 $\log f(x)$ 右边的上界降低为 $\frac{1}{2}(\log x + \log\ln x) + O(1)$.

Erdös 一开始要求 $[0, x]$ 中满足下列条件的整数的最大个数 $k(x)$: 这些数中没有一个能整除任何其他的整数之和. 这种非整除集(nondividing set)显然也是非均值集, 故有 $k(x) \leqslant f(x)$. Straus 证明了 $k(x) \geqslant \max\{f(x/f(x)), f(\sqrt{x})\}$.

Abbott 证明了: 如果 $l(n)$ 是使每个有 n 个数的整数集都包含一个有 m 个数的非均值子集的最大的 m, 那么有 $l(n) > n^{1/13-\varepsilon}$.

请将 C14-16 和 E10-14 加以比较.

参考文献

H. L. Abbott, On a conjecture of Erdős and Straus on non-averaging sets of integers, *Congr. Numer. XV, Proc. 5th Brit. Combin. Conf., Aberdeen*, 1975, 1-4.

H. L. Abbott, Extremal problems on non-averaging and non-dividing sets, *Pacific J. Math.*, **91**(1980) 1-12.

H. L. Abbott, On the Erdős-Straus non-averaging set problem, *Acta Math. Hungar.* **47**(1986) 117-119.

Á. P. Bosznay, On the lower estimation of non-averaging sets, *Acta Math. Hungar.*, **53**(1989) 155-157; *MR* **90d**:11016.

P. Erdős & A. Sárközy, On a problem of Straus, *Disorder in physical systems*, Oxford Univ. Press, New York, 1990, pp. 55-66; *MR* **91i**:11012.

P. Erdős & E. G. Straus, Non-averaging sets II, in *Combinatorial Theory and its Applications* II, *Colloq. Math. Soc. János Bolyai* **4**, North-Holland, 1970, 405-411; *MR* **47** #4804.

E. G. Straus, Non-averaging sets, *Proc. Symp. Pure Math.*, **19**, Amer. Math. Soc., Providence 1971, 215-222.

C17. 最小覆盖问题

令$\{a_i\}$是任一个有 n 个不同整数的集合,$1\leqslant a_i\leqslant 2n$,而$\{b_j\}$是其补集 $1\leqslant b_j\leqslant 2n$, $b_j\neq a_i$. M_k 是$a_i-b_j=k(-2n<k<2n)$的解数,而 $M=\min\max_k M_k$,其中最小值取过所有的序列$\{a_i\}$. Erdös 证明了 $M>n/4$, Scherk 将它改进为 $M>(4-\sqrt{6})n/5$. Leo Moser 得到进一步的改进 $M>\sqrt{2}(n-1)/4$ 和 $M>\sqrt{4-\sqrt{15}}(n-1)$. 在其他的方向上, Motzkin, Ralston 和 Selfridge 得到了满足 $M<2n/5$ 的例子,这和 Erdös 的猜想 $M=\frac{1}{2}n$ 矛盾. 是否存在一个数 c 使得有$M\sim cn$?

Leo Moser 对$\{a_i\}$的基数不是 n 而是k 的情形提出了对应的问题,这里 $k=\lfloor\alpha n\rfloor$, α 是某个实数,$0<\alpha<1$.

一个密切相关的问题属于 J. Czipszer:设 $A_k=\{a_1+k,a_2+k,\cdots,a_n+k\}$(这里 $a_1<a_2<\cdots<a_n$ 是任意的整数且$k\geqslant 0$),设 M_k 是 A_k 的不在 $A-0$ 中的元素个数, $M=\min_{A_0}\max_{0<k\leqslant n}M_k$. Czipszer 证明了 $n/2\leqslant M\leqslant 2n/3$,并猜想 $M=2n/3$. Katz 和 Schnitzer 证明了,对 $n\geqslant 26$ 有 $M>0.6n$. Moser 和 Murdeshwar 考虑了它的连续类似物.

参 考 文 献

P. Erdős, Some remarks on number theory (Hebrew, English summary), *Riveon Lematematika*, **9**(1955) 45–48; *MR* **17**, 460.

M. Katz & F. Schnitzer, On a problem of J. Czipszer, *Rend. Sem. Mat. Univ. Padova* **44**(1970) 85–90; *MR* **45** #8540.

L. Moser, On the minimum overlap problem of Erdős, *Acta Arith.*, **5**(1959) 117–119; *MR* **21** #5594.

L. Moser & M. G. Murdeshwar, On the overlap of a function with its translates, *Nieuw Arch. Wisk.*(3), **14**(1966) 15–18; *MR* **33** #4218.

T. S. Motzkin, K. E. Ralston & J. L. Selfridge, Minimum overlappings under translation, *Bull. Amer. Math. Soc.*, **62**(1956) 558.

S. Swierczkowski, On the intersection of a linear set with the translation of its complement, *Colloq. Math.*, **5**(1958) 185-197; *MR* **21** #1955.

C18. n 个王后问题

在 $n\times n$ 棋盘上最少可以放置多少个王后，使得每个方格或者被一个王后占据，或者受到王后的攻击？Berge 注意到(用图论的语言)这等同于说：在有 64 个顶点的图上求其最小外固集，在该图中仅当两个顶点在同一行、同一列或同一对角线时才是连结的．按照他的记号，对王后有 $\beta=5$ 图 7(a)，对象有 $\beta=8$ 图 7(b)，对马有 $\beta=12$ 图 7(c)．

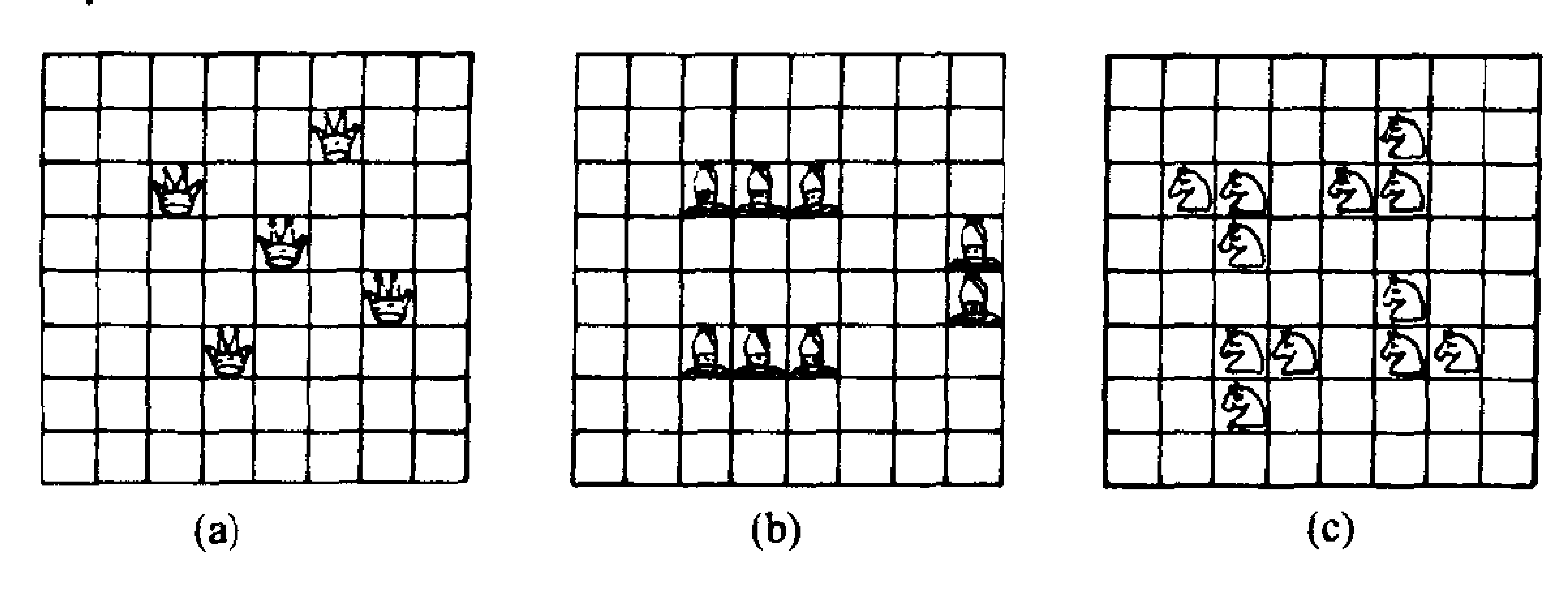


图 7　棋盘用王后、象和马的最小覆盖

虽然并未限制一个棋子不可以保卫另一个棋子，但是图 7 中的王后和象都符合这个限制(即图 7 中的王后和象都不能相互保护——译者注)，而马则不受此限(例如，图 7 中的马 d3 和 c5 可以相互保护——译者注)．由于在国际象棋中棋子不攻击它所在的方格，故而事实上有两组问题．例如，Victor Meally 注意到，如果允许王后相互保护，在 6×6 的棋盘上只要 3 个王后就够了(在 a6，c2，e4 上)，而在 7×7 的棋盘上只要 4 个王后就够了．

在 $n\times n$ 的棋盘上，Kraitchik 对王后给出了下面的表

n	5	6	7	8	9	10	11	12	13	14	15	16	17
王后个数	3	4	5	5	5	5	5	6	7	8	9	9	9

对 $n=5,6,11$，相应的位置画在图 8 中.

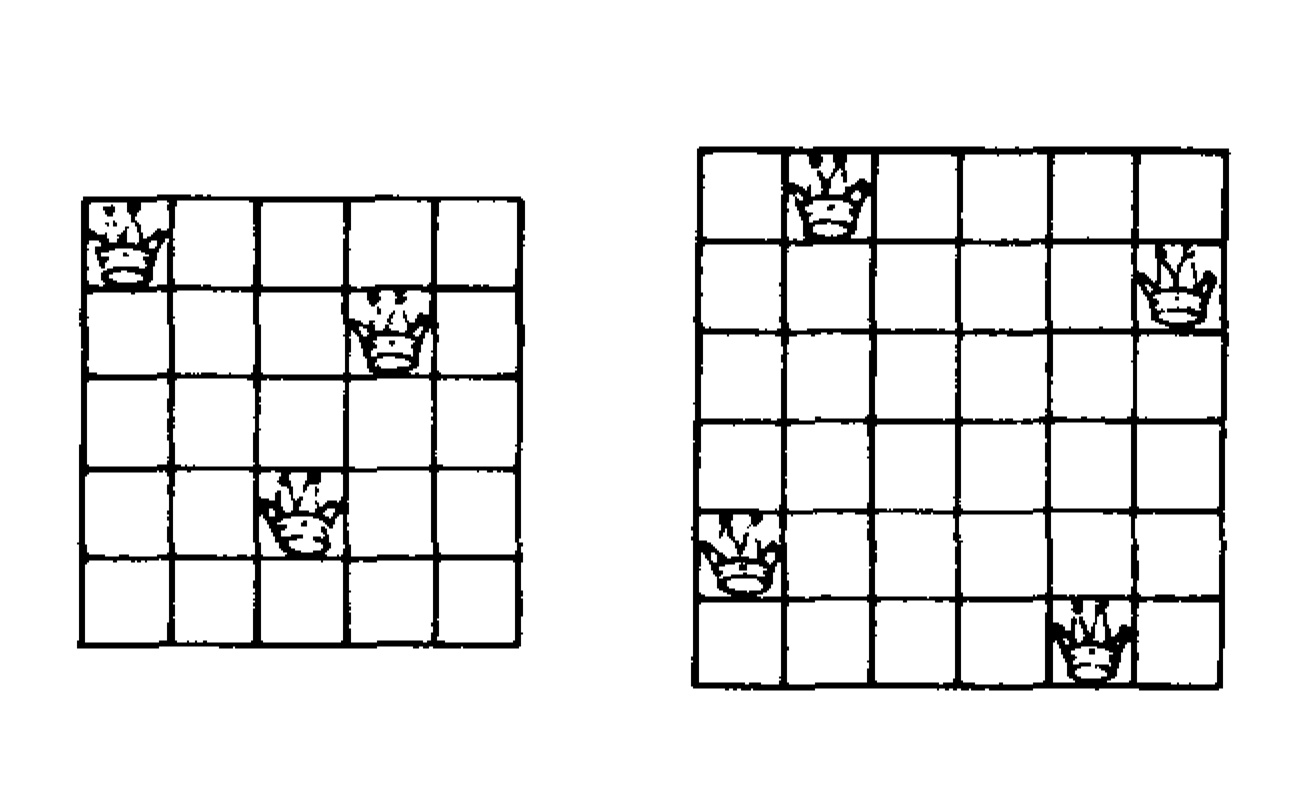
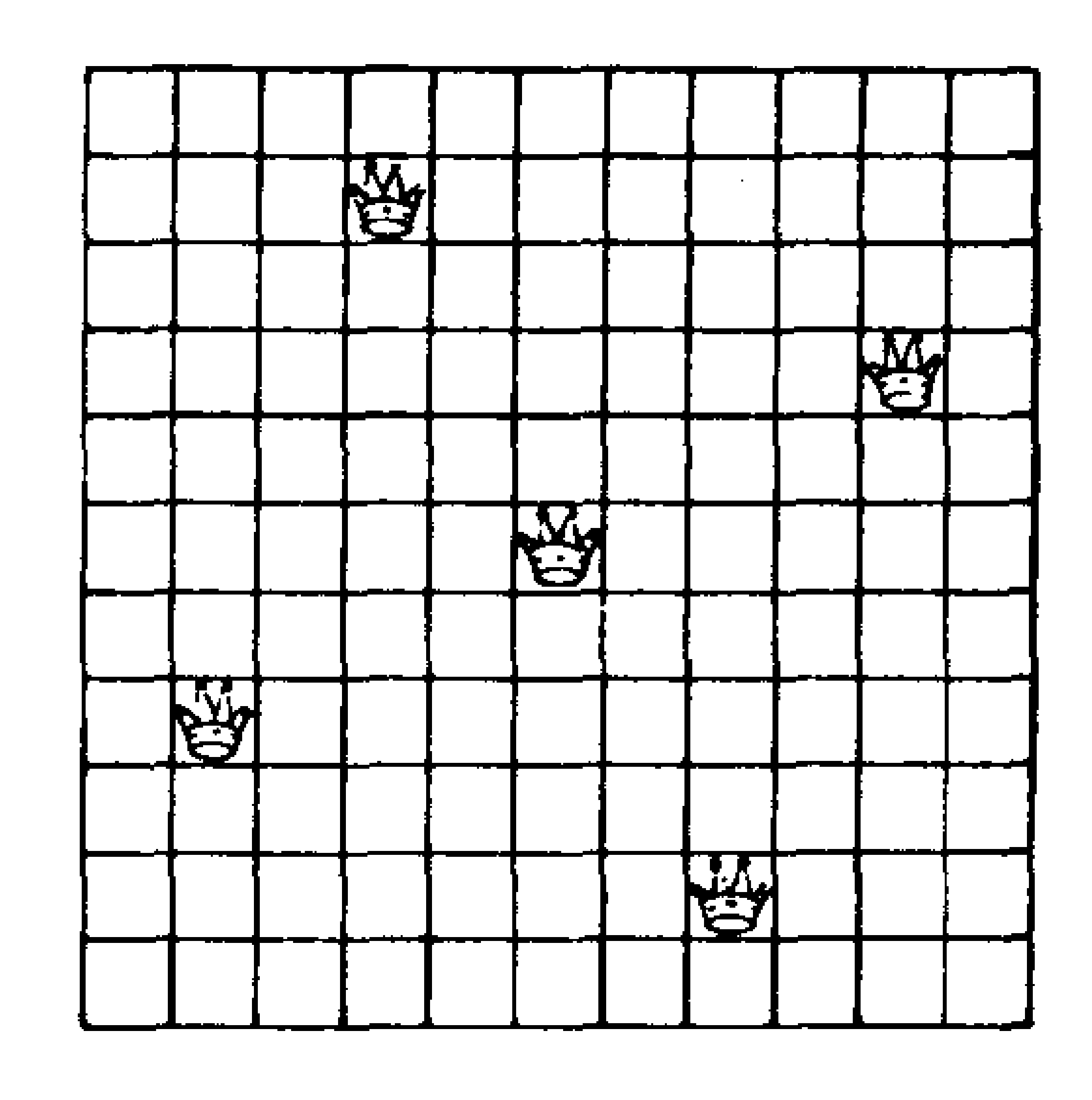



图 8　覆盖 $n\times n$ 棋盘的王后（$n=5,6,11$）

如果我们试图把 1 到 $2n$ 的数分成 n 对 a_i,b_i，使得 $2n$ 个数 $a_i\pm b_i$ 恰好在模 $2n$ 的每个剩余类中有一个，我们会发现那是不可能的. 限制松一些，Shen Mok-Kong 和 Shen Tsen-Pao 要求 $2n$ 个数 $a_i\pm b_i$ 是不同的. 他们给出了下述例子. 对 $n=3$：1，5；2，3；4，6. 对 $n=6$：1，10；2，6；3，9；4，11；5，8；7，12. 对 $n=8$：1，10；2，14；3，16；4，11；5，9；6，12；7，15；8，13；而 Selfridge 证明了对 $n\geqslant 3$ 恒有解. 对每个 n 有多少个解呢？

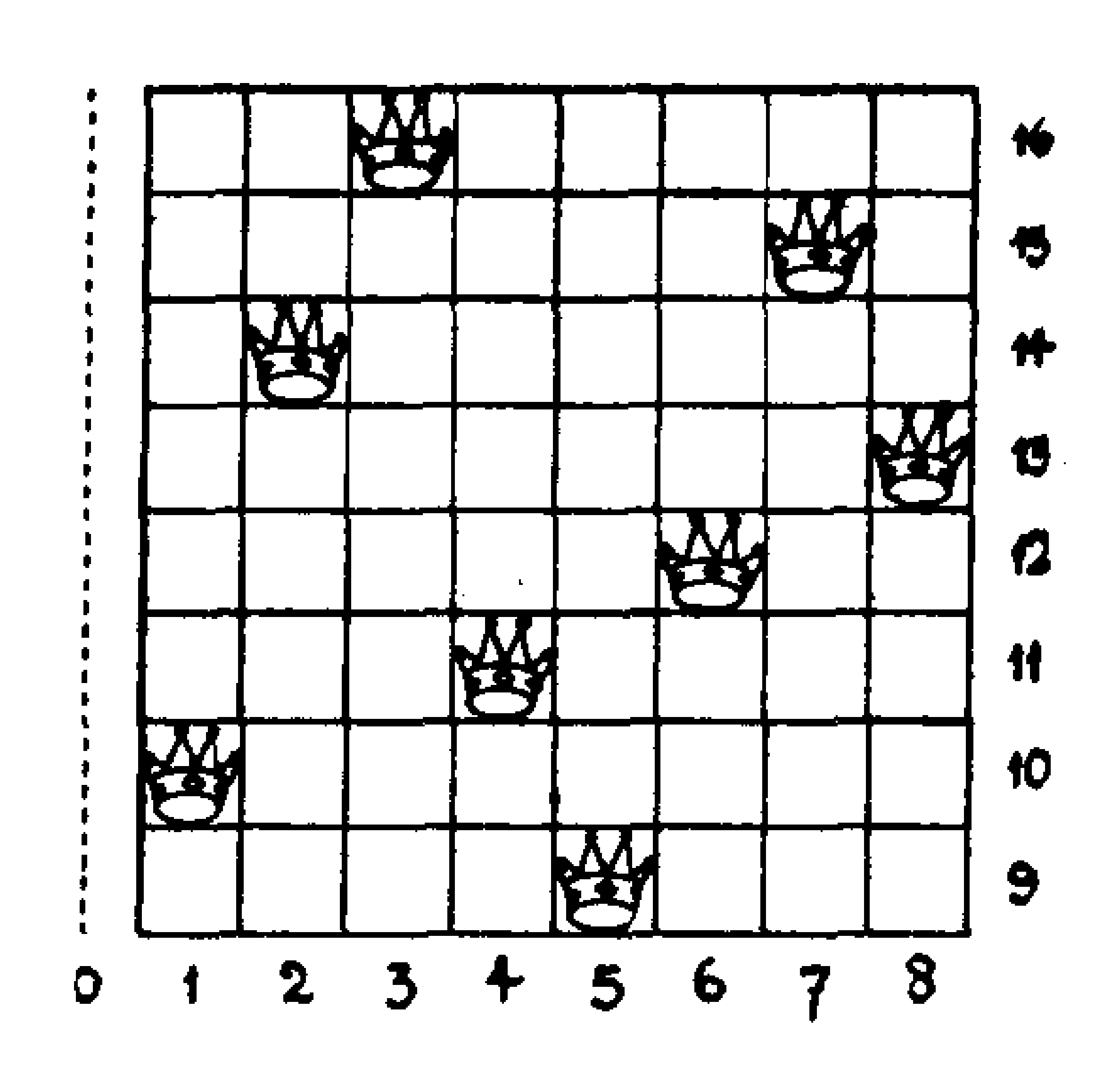


图 9　反射王后问题的一个解

如果加入条件 $b_i=i\,(1\leqslant i\leqslant n)$，我们就得到反射王后问题：在 $n\times n$ 棋盘上放置 n 个王后，使得没有两个王后在同一行、同一列或者同一条对角线上，其中"在对角线上"的含义是指：我们把以第零列的中心所作的镜面反射也包含在内(图 9).

我们可以再次在下述两种情形对每个 n 求其解数：其一是区分由旋转和反射得到的解；其二是对此不加区分.

参考文献

Claude Berge, *Theory of Graphs*, Methuen, 1962, p. 41.

Paul Berman, Problem 122, *Pi Mu Epsilon J.*, **3**(1959-64) 118, 412.

A. Bruen & R. Dixon, The n-queens problem, *Discrete Math.*, **12**(1975) 393–395.

E. J. Cockayne & S. T. Hedetniemi, A note on the diagonal queens domination problem, DM-301-IR, Univ. of Victoria, BC, March 1984.

B. Gamble, B. Shepherd & E. T. Cockayne, Domination of chessboards by queens on a column, DM-318-IR, Univ. of Victoria, BC, July 1984.

Solomon W. Golomb & Herbert Taylor, Constructions and properties of Costas arrays, Dept. Elec. Eng., Univ. S. California, July 1981–Oct. 1983.

B. Hansche & W. Vucenic, On the n-queens problem, *Notices Amer. Math. Soc.*, **20**(1973) A-568.

G. B. Huff, On pairings of the first $2n$ natural numbers, *ActaArith.*, **23**(1973) 117–126.

D. A. Klarner, The problem of the reflecting queens, *Amer. Math. Monthly*, **74**(1967) 953–955; *MR* **40** #7123.

Maurice Kraitchik, *Mathematical Recreations*, Norton, New York, 1942, 247–256.

J. D. Sebastian, Some computer solutions to the reflecting queens problem, *Amer. Math. Monthly*, **76**(1969) 399–400; *MR* **39** #4018.

J. L. Selfridge, Pairings of the first $2n$ integers so that sums and differences are all distinct, *Notices Amer. Math. Soc.*, **10**(1963) 195.

Shen Mok-Kong & Shen Tsen-Pao, Research Problem 39, *Bull. Amer. Math. Soc.*, **68** (1962) 557.

B. Shepherd, B. Gamble & E. T. Cockayne, Domination parameters for the bishops graph, DM-327-IR, Univ. of Victoria, BC, Oct. 1884.

M. Slater, Problem 1, *Bull. Amer. Math. Coc.*, **69**(1963) 333.

P. H. Spencer & E. J. Cockayne, An upper bound for the domination number of the queens graph, DM-376-IR, Univ. of Victoria, BC, June 1985.

Ilan Vardi, Computational Recreations in *Mathematica*©, Addison-Wesley, Redwood City CA, 1991, Chap. 6.

C19. 弱独立序列是强独立序列的有限并集吗?

Selfridge 称一个正整数集合 $a_1<a_2<\cdots<a_k$ 是**独立的**(independent), 如果 $\sum c_i a_i = 0$(其中 c_i 是不全为零的整数) 蕴含至少有一个 $c_i < -1$. 利用抽屉原理易证:如果 k 个正整数是独立的,那么 a_1 至少是 2^{k-1}. 他悬赏 10 美元给解答下列问题者:k 个独立整数 $a_i = 2^k - 2^{k-i}(1 \leqslant i \leqslant k)$ 的集合是最大元素小于 2^k 的惟一集合吗?它是否是这样的集合中使 $a_1 = 2^{k-1}$ 成立的惟一集合?

称一个(无限)正整数序列 $\{a_i\}$ 是**弱独立的**(weakly independent),如果任何关系 $\sum \varepsilon_i a_i = 0$($\varepsilon_i = 0$ 或 ± 1,且除了有限多个非零值外恒有 $\varepsilon_i = 0$)都蕴含 $\varepsilon_i = 0$(对所有 i);又称它为**强独立的**(strongly independent),如果同样的条件对 $\varepsilon_i = 0, \pm 1$, 或 ± 2 为真. Richard Hall 问是否每个弱独立序列都是强独立序列的有限并集?

参考文献

J. L. Selfridge, Problem 123, *Pi Mu Epsilon J.*, 3(1959-64) 118, 413–414.

C20. 平 方 和

Paul Turán 要求对可以表为 4 个两两互素的平方数之和的那些正整数 n,即 $n = x_1^2 + x_2^2 + x_3^2 + x_4^2, x_i \perp x_j (1 \leqslant i < j \leqslant 4)$ 的特征予以刻画. Leech 注意到,诸 x_i 中至多有一个是偶的,从而有 $n \equiv 3,4,7 \bmod 8$. 类似地,$n \equiv 2 \bmod 3$ 不能有这样的表示.

Turán 还猜想:所有正整数都可以表为至多 5 个两两互素的平方数之和,但是 Mąkowski(见问题 B5 的文献)发现数 $4^k(24l+15)(k \geqslant 2)$不能用这种方式表示. 有任意大的整数不能恰好用 5 个互素的平方数之和来表示,这是因为 $3n = x_1^2 + \cdots + x_5^2$ 蕴含 3 整除诸 x_i 中的两个. 事实上,两个形如 $24k+7$ 的不同素数之积

不能表为少于 10 个两两互素的平方数之和，Leech 问是否这是最好可能的结果？

除了 256 个例子外(其中最大的一个是 1167)，每个数均可表为至多 5 个合数的平方之和.

Chowla 猜想每个正整数都是集合 $\{(p^2-1)/24\}$ (其中 $p \geq 5$ 为素数)中至多 4 个元素之和. 要求用 4 个这样的加数来表示的最小的数是 33.

试把这些问题和 Wright 早先的结果相比较，例如 Wright 证明了：如果 $\lambda_1, \cdots, \lambda_4$ 是给定的实数，其和为 1，那么每个有一个充分大的奇数因子的数 n 皆可表成 $n = m_1^2 + \cdots + m_4^2$，其中 $|m_i^2 - \lambda_i n| = o(n)$. 对 5 个或更多的平方和，以及对 3 个平方和(当然，在最后一种情形只要 n 不是形如 $4^k(8l+7)$ 的数)，他也有类似的结果.

Bohman，Fröberg 和 Riesel 证明了恰有 31 个数不能表为不同的平方数之和，所有大于 188 的数都可以表为至多 5 个不同的平方数之和. 只有两个数 124 和 188 需要 6 个不同的平方数. 这些结果隐含在 Gordon Pall 的定理 3 中以及 Sprague 的论文中，Sprague 的论文给出了有关任何幂的更一般的结果. 如果要求恰好是多少个平方数之和的话，则 Halter-Koch 证明了，每个大于 412 且不被 8 整除的数都是 4 个不同的非零的平方数之和，每个大于 157 的奇整数也可如此表示. 他还证明了，每个大于 245 的整数是 5 个不同的非零的平方数之和，每个大于 333 的整数是 6 个这样的平方数之和，每个大于 390 的整数是 7 个这样的平方数之和，每个大于 462 的整数是 8 个这样的平方数之和，等等，一直到所有大于 1036 的整数是 12 个这样的平方数之和. Bateman，Hildebrand 和 Purdy 对 Halter-Koch 的论文又写出一个续篇.

用 s_n 表示不能表示成不同的正整数的 n 次幂之和的最大整数. Sprague 证明了 $s_2 = 128$；Graham 说他得到 $s_3 = 12758$；Lin Shen 用他的方法得到 $s_4 = 5134240$. Cam Patterson 用他的筛法和 Richert 的一个结果得到 $s_5 = 67898771$.

Štefan Porubský 利用 Cassels 的一个结果对 R. E. Dressler 的一个问题给出了肯定的回答:对每个正整数 k,每个充分大的正整数都是不同的素数的 k 次幂之和.

我们还可以要求每个数用尽可能少的各种多角形数之和来表示. 例如在 Gauss 1796 年 7 月 10 日的日记中记下了:

$$\text{EΥPHKA!}\quad \text{num} = \triangle + \triangle + \triangle,$$

即每个数可表为 3 个三角数之和. 对六角形数 $r(2r-1)$,如果允许秩(这里数 r 定义为秩——译者注)为负的六角形数 $r(2r+1)$ 出现,则问题有同样的答案;但是如果不允许取秩为负的六角形数,那么 11 和 26 就需要秩为正数的 6 个六角形数来表示. 是否可能每个充分大的数都可以表为 3 个这样的数的和? 等价地说,每个充分大的数 $8n+3$ 是否可以表为 3 个形如 $4r-1$(r 是正数)的数的平方之和? 对五角形数 $\frac{1}{2}r(3r-1)$,相应的问题是:是否每个充分大的形如 $24n+3$ 的数都可以表为 3 个形如 $6r-1$ 的数的平方之和?

参考文献

G. E. Andrews, EΥPHKA! num $= \triangle + \triangle + \triangle$, *J. Number Theory*, **23**(1986) 285–293.

Paul T. Bateman, Adolf Hildebrand & George B. Purdy, Expressing a positive integer as a sum of a given number of distinct squares of positive integers, *Acta Arith.*, (see Abstract 882-11-136, *Abstracts Amer. Math. Soc.*, **14**(1993) 420).

Jan Bohman, Carl-Erik Fröberg & Hans Riesel, Partitions in squares, *BIT*, **19**(1979) 297–301; *MR* **80k**:10043.

J. W. S. Cassels, On the representation of integers as the sums of distinct summands taken from a fixed set, *Acta Sci. Math. Szeged*, **21**(1960) 111–124.

John A. Ewell, On sums of triangular numbers and sums of squares, *Amer. Math. Monthly*, **99**(1992) 752–757; *MR* **93j**:11021.

R. L. Graham, Complete sequences of polynomial values, *Duke Math. J.*, **31**(1964) 275–285.

Andrew Granville & Zhu Yi-Liang, Representing binomial coefficients as sums of squares, *Amer. Math. Monthly*, **97**(1990) 486–493.

Emil Grosswald & L. E. Mattics, Solutions to problem E 3262, *Amer. Math.*

Monthly, **97**(1990) 240–242.

Richard K. Guy, Every number is expressible as the sum of how many polygonal numbers? *Amer. Math. Monthly*, **101**(1994) 169–172.

F. Halter-Koch, Darstellung natürliche Zahlen als Summe von Quadraten, *Acta Arith.*, **42**(1982) 11–20; *MR* **84b**:10025.

Lin Shen, Computer experiments on sequences which form integral bases, in J. Leech (editor) *Computational Problems in Abstract Algebra*, 365–370, Pergamon, 1970.

G. Pall, On sums of squares, *Amer. Math. Monthly*, **40**(1933) 10–18.

Cameron Douglas Patterson, *The Derivation of a High Speed Sieve Device*, PhD thesis, The Univ. of Calgary, March 1992.

V. A. Plaksin, Representation of numbers as a sum of four squares of integers, two of which are prime, *Soviet Math. Dokl.*, **23**(1981) 421–424; transl. of *Dokl. Akad. Nauk SSSR*, **257**(1981) 1064–1066; *MR* **82h**:10027.

Štefan Porubský, Sums of prime powers, *Monatsh. Math.*, **86**(1979) 301–303.

H. E. Richert, Über zerlegungen in paarweise verschiedene zahlen, *Norsk Mat. Tidskrift*, **31**(1949) 120–122.

R. P. Sprague, Über zerlegungen in ungleiche Quadratzahlen, *Math. Z.*, **51** (1949) 289–290; *MR* **10** 283.

R. P. Sprague, Über zerlegungen in n-te Potenzen mit lauter verschiedenen Grundzahlen, *Math. Z.*, **51**(1948) 466–468; *MR* **10** 514.

E. M. Wright, The representation of a number as a sum of five or more squares, *Quart. J. Math. Oxford*, **4**(1933) 37–51, 228–232.

E. M. Wright, The representation of a number as a sum of four 'almost proportional' squares, *Quart. J. Math. Oxford*, **7**(1936) 230–240.

E. M. Wright, Representation of a number as a sum of three or four squares, *Proc. London Math. Soc.*(2), **42**(1937) 481–500.

D. 不定方程

"是这样一门学科:它可以简要地说成其大部分内容是讨论整系数多项式方程 $f(x_1,x_2,\cdots,x_n)=0$ 的有理解或整数解. 广为人知的是,许多世纪以来,还从未有别的哪个论题能吸引如此众多的职业数学家和业余数学家双方的关注,产生出如此大量已发表的论文."

这段出自 Mordell 的书 *Diophantine Equations*(《不定方程》, Academic Press, London, 1969)中的引文指出,这一节里的材料比其他任何章节里的材料选自更多来源不同的资料. 如果你对所述论题感兴趣,请参考 Mordell 的书,该书对已知的结果给出了彻底而清晰的讨论,同时还附有许多未解决的问题. 对代数曲线上的有理点已经有发展得很好的理论,故而我们主要限于讨论更高维的情形,对此种情形尚未发展出标准的方法.

D1. 等幂和,Euler 猜想

"对许多几何学家来说,这个定理(Fermat 定理)似乎可以加以推广. 正如不存在两个立方体,其和或差也是一个立方体一样,可以肯定的是不可能给出 3 个四方数,使它们的和也是一个四方数,但是若要求它们的和是一个四方数的话,这至少需要 4 个四方数,尽管至今尚无人能够给出 4 个这样的四方数. 同样地,似乎也不可能给出 4 个五方数,使它们的和也是一个五方数,对更高次幂也有类似的结果."

直到 1911 年以前,对 Euler 的命题没有做出任何进展,而在 1911 年 R. Norrie 给出了 4 个这样的四方数:

$$30^4+120^4+272^4+315^4=353^4.$$

55 年以后,Lander 和 Parkin 对 Euler 的更一般的猜想给出了一个反例:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

现在已广为人知的是,Noam Elkies 推翻了关于四次幂的 Euler 猜想,因为他的发现已经上了全国性的报纸. 有一族无穷多个解来自 Dem'janenko 给出的 $x^4 - y^4 = z^4 + t^2$ 的参数解中由 $u = -5/8$ 给出的椭圆曲线,解族中的第一个是

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

与 $u = -9/20$ 对应的最小的解

$$95800^4 + 217519^4 + 414560^4 = 422481^4$$

是后来由 Roger Frye 发现的. 有无穷多个 u 的值给出正秩的椭圆曲线和进一步的解族.

Jan Kubiček 的解使 3 个立方的和仍是一个立方,它恰与 F. Vieta 的结果重复(见 Dickson 的书 *History of the Theory of Numbers*[A17],第二卷 pp. 550~551).

Simcha Brudno 问了下面的问题:是否有 $a^5 + b^5 + c^5 + d^5 = e^5$ 的参数解(上面的解是满足 $e \leqslant 765$ 的仅有的一个解)? $a^4 + b^4 + c^4 + d^4 = e^4$ 是否有参数解? 对高于 5 次的幂有 Euler 猜想的反例吗? $a^6 + b^6 + c^6 + d^6 + e^6 = f^6$ 有解吗? 虽然对 $s = 4$ 和 5 方程 $a_1^s + \cdots + a_{s-1}^s = b^s$ 有解,但是对 $n \geqslant 6$,即使是方程 $a_1^s + \cdots + a_s^s = b^s$ 也没有已知的解.

对同样个数的相等的等幂和

$$\sum_{i=1}^{m} a_i^s = \sum_{i=1}^{m} b_i^s$$

$(a_i > 0, b_i > 0)$,当 $2 \leqslant s \leqslant 4$ 和 $m = 2$ 以及当 $s = 5, 6$ 和 $m = 3$ 已知它有参数解. 对 $s = 7$ 和 $m = 4$ 能找到它的数值解吗? 对 $s = 5$ 和 $m = 2$ 还不知道是否有 $a^5 + b^5 = c^5 + d^5$ 的非平凡解存在. Dick Lehmer 曾认为可能有一个解,其和大约是一个 25 位的数. 但是在解的和 $\leqslant 1.02 \times 10^{26}$ 的范围内 Blair Kelly III 没有搜索到非平凡的解.

"Hardy-Ramanujan 数"$1729 = 1^3 + 12^3 = 9^3 + 10^3$ 首先于 1657 年由 Bernard Frénicle de Bessy 发现;1957 年 Leech 发现了

$$87539319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3.$$

而最近 Rosenstiel, Dardis 和 Rosenstiel 发现了

$$\begin{aligned} 6963472309248 &= 2421^3 + 19083^3 = 5436^3 + 18948^3 \\ &= 10200^3 + 18072^3 = 13322^3 + 15530^3. \end{aligned}$$

Hardy 和 Wright 的书中的定理 412 表明,这种和的个数可以做到任意大,但是对于 5 个或更多的等幂和,并不知道最小的例子. 如果允许取负整数,Randall Rathbun 补充了如下的例子:

$$\begin{aligned} 6017193 &= 166^3 + 113^3 = 180^3 + 57^3 = 185^3 - (68)^3 \\ &= 209^3 - (146)^3 = 246^3 - (207)^3 \\ 1412774811 &= 963^3 + 804^3 = 1134^3 - (357)^3 = 1155^3 - (504)^3 \\ &= 1246^3 - (805)^3 = 2115^3 - (2004)^3 \\ &= 4746^3 - (4725)^3 \\ 11302198488 &= 1926^3 + 1608^3 = 1939^3 + 1589^3 \\ &= 2268^3 - (714)^3 = 2310^3 - (1008)^3 \\ &= 2492^3 - (1610)^3 = 4230^3 - (4008)^3 \\ &= 9492^3 - (9450)^3. \end{aligned}$$

Mordell 和 Mahler 证明了,$n = x^3 + y^3$ 的解数能 $> c(\ln n)^{\alpha}$,而 Silverman 将他们的结果中 α 的值从$\frac{1}{4}$改进为$\frac{1}{3}$,并且证明了:如果要求每对立方数互素,那么存在常数 c 使得这样的解的个数 $< c^{r(n)}$,这里 $r(n)$是椭圆曲线 $x^3 + y^3 = n$ 的秩. 求这些解一定更加困难. 到目前为止找到的最大的表法个数是 1983 年由 P. Vojta给出的 3:

$$15170835645 = 517^3 + 2468^3 = 709^3 + 2456^3 = 1733^3 + 2152^3,$$

不过今天人的洞察力和计算能力可能会很快打破此项记录. 如果允许取负整数的话,Randall Rathbun 给出了无立方因子数的例子:

$$16776487 = 220^3 + 183^3 = 255^3 + 58^3$$

$$=256^3+(-9)^3=292^3+(-201)^3.$$

数 1729 也是第三个 Carmichael 数(见 A13),Pomerance 观察到:第二个 Carmichael 数 1105 可以比任何更小的数用更多的方式表为两个平方数之和. Granville 邀请读者对第一个 Carmichael 数 561 给出相应的结论.

Euler 知道 $635318657=133^4+134^4=59^4+158^4$,Leech 证明了这是最小的例子. 还无人知道有 3 个这样相等的和.

已知生成 $a^4+b^4=c^4+d^4$ 的参数解的一种方法,它可以生成从平凡的解$(\lambda,1,\lambda,1)$开始的所有已发表的解. 它将只产生阶为 $6n+1$ 的解. 在此,为回答 Brudno 的一个问题,要求 $6n+1$ 是一个素数. 虽然阶 25 不出现,但是阶 49 出现. 最近,Ajai Choudhry 找到了阶 25 的一个参数解.

Swinnerton-Dyer 有第二个方法可以从老的解生成新的解,他能证明:这两个方法加上对称性可以生成所有非奇异的参数解,即与无奇点的曲线上的点对应的所有的解(由齐次方程 $F(x,y,z)=0$ 给出的曲线上的点称为是奇异的(singular),如果恰有 $\frac{\partial F}{\partial x}=\frac{\partial F}{\partial y}=\frac{\partial F}{\partial z}=0$.). 此外,在下述意义下这个程序还是构造性的:他可以给出一个有限程序来求出所有给定阶的非奇异解. 所有非奇异解都是奇数阶的,且所有充分大的奇数阶一定出现. 然而令人遗憾的是总有奇解存在. Swinnerton-Dyer 有一个方法生成奇解,但是没有理由相信它可以给出全部奇解. 描述所有奇解需要全新的思想. 有些奇解有偶数阶,他猜想(且有可能证明)所有充分大的偶数阶都以这种方式出现.

在同样的意义下,Andrew Bremner 能找到 $a^6+b^6+c^6=d^6+e^6+f^6$ 的"所有的"参数解,它们也满足方程

$$a^2+ad-d^2=f^2+fc-c^2$$
$$b^2+be-e^2=d^2+da-a^2$$
$$c^2+cf-f^2=e^2+eb-b^2$$

(这并非像初看起来的那样一种限制). $a^6+b^6+c^6=d^6+e^6+f^6$的许多解也满足 $a^2+b^2+c^2=d^2+e^2+f^2$,而且这两个方程的所有已知的联立解(带有适当的符号)也满足上面三个方程,例如由 Subbarao 发现的最小的解 $(a,b,c,d,e,f)=(3,9,22,-23,10,-15)$. 有反例存在吗? Peter Montgomery 列举出 18 个相等的 3 个六次幂和,其相应的平方和并不相等,其中最小的是

$$25^6+62^6+138^6=82^6+92^6+135^6.$$

Bremner 也能找到 $a^5+b^5+c^5=d^5+e^5+f^5$ 的"所有"参数解,这些解也满足 $a+b+c=d+e+f$ 和 $a-b=d-e$.

Bob Scher 称一个和 $\sum_{i=1}^{m} a_i^p=0$(这里 p 是素数)是"完全的",如果对任何 a_i,总有惟一的 a_i' 存在,使有 $a_i+a_i'\equiv 0 \bmod p$. 如果 $a_i\equiv 0 \bmod p$,则有 $a'_i=a_i$. 他指出,如果 $p=3$ 且 $m<9$ 或者 $p=5$ 且 $m<7$,那么每个这样的和都是完全的.

人们对联立方程

$$a^n+b^n+c^n=d^n+e^n+f^n$$
$$a^nb^nc^n=d^ne^nf^n$$

有某种兴趣. 对 $n=2$,问题至少可追溯到 Bini,而 Dubouis 和 Mathieu 也给出了部分解;真正一般性的解最近由 John B. Kelly 给出. Stephane Vandemergel 对 $n=3$ 找到 62 个解,对 $n=4$ 找到 3 个解:(29,66,124;22,93,116),(54,61,196;28,122,189)和(19,217,657;9,511,589). 他注意到,如果 $r^n+s^n=u^n+v^n$,则 $(ru,su,v^2;rv,sv,u^2)$是一个解,这表明对 $n\leqslant 4$ 有无穷多个解. 他的解中大多数都不是这种形式.

Tarry-Escott 问题有值得注意的历史(见 Dickson 的书[A17],第二卷第 24 章),有一本 Gloden 写的关于多级方程(multigrade equation)(组)

$$\sum_{i=1}^{l} n_i^j=\sum_{i=1}^{l} m_i^j \qquad (j=1,2,\cdots,k)$$

的书. 对于 $k=9,l=10$ 的一个引人注目的例子属于 Letac,其中

$(n_i, m_i) = \pm 12, \pm 11881, \pm 20231, \pm 20885, \pm 23738; \pm 436, \pm 11857, \pm 20449, \pm 20667, \pm 23750$. Smyth 指出,这是一族无穷多个独立解中的一项.

参考文献

U. Bini, Problem 3424, *L'Intermédiaire des Math.*, **15**(1908) 193.

B. J. Birch & H. P. F. Swinnerton-Dyer, Notes on elliptic curves, II, *J. reine angew. Math.*, **218**(1965) 79–108.

Andrew Bremner, Pythagorean triangles and a quartic surface, *J. reine angew. Math.*, **318**(1980) 120–125.

Andrew Bremner, A geometric approach to equal sums of sixth powers, *Proc. London Math. Soc.*(3), **43**(1981) 544–581; *MR* **83g**:14018.

Andrew Bremner, A geometric approach to equal sums of fifth powers, *J. Number Theory*, **13**(1981) 337–354; *MR* **83g**:14017.

Andrew Bremner & Richard K. Guy, A dozen difficult Diophantine dilemmas, *Amer. Math. Monthly*, **95**(1988) 31–36.

S. Brudno, Some new results on equal sums of like powers, *Math. Comput.*, **23**(1969) 877–880.

S. Brudno, On generating infinitely many solutions of the diophantine equation $A^6 + B^6 + C^6 = D^6 + E^6 + F^6$, *Math. Comput.*, **24**(1970) 453–454.

S. Brudno, Problem 4, *Proc. Number Theory Conf. Univ. of Colorado*, Boulder, 1972, 256–257.

Simcha Brudno, Triples of sixth powers with equal sums, *Math. Comput.*, **30**(1976) 646–648.

S. Brudno & I. Kaplansky, Equal sums of sixth powers, *J. Number Theory*, **6**(1974) 401–403.

Ajai Choudhry, The Diophantine equation $A^4 + B^4 = C^4 + D^4$, *Indian J. Pure Appl. Math.*, **22**(1991) 9–11; *MR* **92c**:11024.

Ajai Choudhry, Symmetric Diophantine systems, *Acta. Arith.*, **59**(1991) 291–307; *MR* **92g**:11030.

Jean-Joël Delorme, On the Diophantine equation $x_1^6 + x_2^6 + x_3^6 = y_1^6 + y_2^6 + y_3^6$, *Math. Comput.*, **59**(1992) 703–715; *MR* **93a**:11023.

V. A. Dem'janenko, L. Euler's conjecture (Russian), *Acta Arith.*, **25**(1973/74) 127–135; *MR* **50** #12912.

Dubouis & Mathieu, Réponse 3424, *L'Intermédiaire des Math.*, **16**(1909) 41–42, 112.

Noam Elkies, On $A^4+B^4+C^4 = D^4$, *Math. Comput.*, **51**(1988) 825–835; and see Ivars Peterson, *Science News*, **133**, #5(88-01-30) 70; Barry Cipra, *Science*, **239**(1988) 464; and James Gleick, *New York Times*, 88-04-17.

A. Gérardin, *L'Intermédiare des Math.*, **15**(1908) 182; *Sphinx-Œdipe*, 1906-07 80, 128.

A. Gloden, *Mehrgradige Gleichungen*, Noordhoff, Groningen, 1944.

John B. Kelly, Two equal sums of three squares with equal products, *Amer.

Math. Monthly, **98**(1991) 527–529; *MR* **92j**:11025.
Jan Kubiček, A simple new solution to the diophantine equation $A^3+B^3+C^3=D^3$ (Czech, German summary), *Časopis Pěst. Mat.*, **99**(1974) 177–178.
L. J. Lander, Geometric aspects of diophantine equations involving equal sums of like powers, *Amer. Math. Monthly*, **75**(1968) 1061–1073.
L. J. Lander & T. R. Parkin, Counterexample to Euler's conjecture on sums of like powers, *Bull. Amer. Math. Soc.*, **72**(1966) 1079; *MR* **33** #5554.
L. J. Lander, T. R. Parkin & J. L. Selfridge, A survey of equal sums of like powers, *Math. Comput.*, **21**(1967) 446–459; *MR* **36** #5060.
Leon J. Lander, Equal sums of unlike powers, *Fibonacci Quart.*, **28**(1990) 141–150; *MR* **91e**:11033.
John Leech, Some solutions of Diophantine equations, *Proc. Cambridge Philos. Soc.* **53**(1957) 778–780; *MR* **19** 837f.
R. Norrie, in University of Saint Andrews 500th Anniversary Memorial Volume of Scientific Papers, published by the University of St. Andrews, 1911, 89.
E. Rosenstiel, J. A. Dardis & C. R. Rosenstiel, The four least solutions in distinct positive integers of the Diophantine equation $s=x^3+y^3=z^3+w^3=u^3+v^3=m^3+n^3$, *Bull. Inst. Math. Appl.*, **27**(1991) 155–157; *MR* **92i**:11134.
Joseph H. Silverman, Integer points on curves of genus 1, *J. London Math. Soc.*(2), **28**(1983) 1–7; *MR* **84g**:10033.
Joseph H. Silverman, Taxicabs and sums of two cubes, *Amer. Math. Monthly*, **100**(1993) 331–340; *MR* **93m**:11025.
C. J. Smyth, Ideal 9th-order multigrades and Letac's elliptic curve, *Math. Comput.*, **57**(1991) 817–823.
K. Subba-Rao, On sums of sixth powers, *J. London Math. Soc.*, **9**(1934) 172–173.
Ju. D. Trusov, New series of solutions of the thirty second problem of the fifth book of Diophantus (Russian). *Ivanov. Gos. Ped. Inst. Učen. Zap.*, **44**(1969) 119–121 (and see 122–123); *MR* **47** #4925(-6).
Morgan Ward, Euler's three biquadrate problem, *Proc. Nat. Acad. Sci. U.S.A.*, **31**(1945) 125–127; *MR* **6**, 259.
Morgan Ward, Euler's problem on sums of three fourth powers, *Duke Math. J.*, **15**(1948) 827–837; *MR* **10**, 283.
A. S. Werebrusow, *L'Intermédiare des Math.*, **12**(1905) 268; **25**(1918) 139.
Aurel J. Zajta, Solutions of the diophantine equation $A^4+B^4=C^4+D^4$, *Math. Comput.*, 41(1983) 635–659.

D2. Fermat 问题

看来 Fermat 大定理对奇素数 p,方程

$$x^p + y^p = z^p$$

不可能有正整数解最终确实要成为一个定理了. 但是它的证明很

长，而且还要依赖其他人的工作．的确，正当我在写作本书时，有消息说在它的证明中发现了一个漏洞，这个漏洞有可能加以修补，但“可能要花一两年时间．”(这一漏洞已经于1995年获得解决，从而历经300多年的这一著名猜想终于获得解决．有关Fermat大定理的证明参见以下文献：A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141** (1995), 443～551; R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553～572.——译者注)Ribet 指出：Fermat 定理可以从关于椭圆曲线的 Taniyama-Weil 猜想推出．由于这里的篇幅所限，不能给出更多的证明，有关内容见B19．这提出了如下的哲学问题：我们已经耗尽了“理性的”证明，而必须教会计算机来为我们检查结果吗？

Kummer 对所有正则素数证明了该定理，这里一个素数 p 称为是正则的(regular)，如果它不整除分圆域 $Q(\zeta_p)$ 中等价理想类的个数 h_p．他还证明了：一个素数是正则的，仅当它不整除 Bernoulli 数(Bernoulli number) $B_2, B_4, \cdots, B_{p-3}$ 的分子，其中

$$B_{2k} = (-1)^{k-1}\frac{2(2k)!}{(2\pi)^{2k}}\zeta(2k)$$

$\left(\zeta(2k) = \sum_{n=1}^{\infty} n^{-2k}\text{，见 A17}\right)$．在小于 10^6 的 78497 个素数中，有 47627 个是正则的，这和猜想的正则素数的密度 $e^{-1/2}$ 相当吻合．然而，甚至尚未证明有无穷多个正则素数．另一方面，Jensen 证明了有无穷多个非正则素数．素数 $p = 16843$ 整除 B_{p-3}，Richard McIntosh 以及 Buhler, Crandall, Ernvall 和 Metsänkylä 都注意到，这对 $p = 2124679$ 也为真．

在本书第一版中提到的 J. M. Gandhi 的某些辅助性的问题可以由 Wiles 的方法来解决(如果它经受住仔细审查的考验的话)，这一方法表明，如果 $p \geqslant 11$ 且 γ 是诸素数 3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59, …中某一个的幂，则

$$x^p + y^p + \gamma z^p = 0$$

不可解.

对什么样的整数 c, $x^4+y^4=cz^4$ 有满足 $x\perp y$ 且 $z>1$ 的整数解? Leech 给出一种方法来求任何 $z=a^4+b^4$ 的非平凡解:他找到的最小的解是 $25^4+149^4=5906\cdot 17^4$. Bremner 和 Morton 指出:5906 是能表为两个有理数的四次幂之和但不是两个整数的四次幂之和的最小整数.

证明 $x^n+y^n=n!z^n$ 没有满足 $n>2$ 的整数解. Erdös 和 Obláth 证明了: $x^p\pm y^p=n!$ 没有满足 $p>2$ 的解,而 Erdös 说 $x^4+y^4=n!$ 没有满足 $x\perp y$ 的解. 的确,即使没有最后这个条件,Leech 也发现:对 $n>3$,在区间 $[n+1,2n]$ 中有一个素数 $\equiv 3 \bmod 4$,于是对 $n>6$ 就有 $n!$ 的一个单重(不是多重)素因子,因此对 $n>6$, $n!$ 甚至不是两个平方数之和(除了 $n=0,1,2$ 以外,仅有的解是 $6!=24^2+12^2$)(与 D25 比较).

Granville 的论文(评论者在该文中感受到一种新的强有力的思想的涌动)已经把 Fermat 问题和许多其他的猜想(包括 *ABC* 猜想(B19)以及 Erdös 的幂数猜想(B16))联系在了一起.

参考文献

Andrew Bremner & Patrick Morton, A new characterization of the integer 5906, *Manuscripta Math.*, **44**(1983) 187–229; *MR* **84i**:10016.

J. P. Buhler, R. E. Crandall & R. W. Sompolski, Irregular primes to one million, *Math. Comput.*, **59**(1992) 717–722; *MR* **93a**:11106.

J. P. Buhler, R. E. Crandall, R. Ernvall & T. Metsänkylä, Irregular primes and cyclotomic invariants to four million, *Math. Comput.*, **61**(1993) 151–153; *MR* **93k**:11014.

M. Chellali, Accélération de calcul de nombres de Bernoulli, *J. Number Theory*, **28**(1988) 347–362.

Don Coppersmith, Fermat's last theorem (case 1) and the Wieferich criterion, *Math. Comput.*, **54**(1990) 895–902; *MR* **90h**:11024.

Harold M. Edwards, *Fermat's Last Theorem, a Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, New York, 1977.

P. Erdős & R. Obláth, Über diophantische Gleichungen der form $n!=x^p\pm y^p$ and $n!\pm m!=x^p$, *Acta Litt. Sci. Szeged*, **8**(1937) 241–255; *Zbl.* **17**.004.

Andrew Granville, Some conjectures related to Fermat's last theorem, *Number Theory* (*Banff*), 1988, de Gruyter, 1990, 177–192; *MR* **92k**:11036.

Andrew Granville, Some conjectures in analytic number theory and their connection with Fermat's last theorem, in *Analytic Number Theory* (*Proc. Conf. Honor Bateman*, 1989), Birkhäuser, 1990, 311–326; *MR* **92a**:11031.

K. Inkeri & A. J. van der Poorten, Some remarks on Fermat's conjecture, *Acta Arith.*, **36**(1980) 107-111.

Wells Johnson, Irregular primes and cyclotomic invariants, *Math. Comput.*, **29** (1975) 113-120; *MR* **51** #12781.

D. H. Lehmer, E. Lehmer & H. S. Vandiver, An application of high-speed computing to Fermat's Last Theorem, *Proc. Nat. Acad. Sci. U.S.A.*, **40**(1954), 25–33.

Paulo Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, Heidelberg, Berlin, 1979; see *Bull. Amer. Math. Soc.*, **4**(1981) 218–222; *MR* **81f**:10023.

K. Ribet, On modular representations of Gal($^-$**Q**/**Q**) arising from modular forms, *Invent. Math.*, **100**(1990) 431–476.

J. L. Selfridge, C. A. Nicol & H. S. Vandiver, Proof of Fermat's last theorem for all prime exponents less than 4002, *Proc. Nat. Acad. Sci., U.S.A.* **41**(1955) 970–973; *MR* **17**, 348.

Daniel Shanks & H.C. Williams, Gunderson's function in Fermat's last theorem, *Math. Comput.*, **36**(1981) 291–295.

R. W. Sompolski, The second case of Fermat's last theorem for fixed irregular prime exponents, Ph.D. thesis, Univ. Illinois Chicago, 1991.

Jonathan W. Tanner & Samuel S. Wagstaff, New bound for the first case of Fermat's last theorem, *Math. Comput.*, **53**(1989) 743–750; *MR* **90h**:11028.

Samuel S. Wagstaff, The irregular primes to 125000, *Math. Comput.*, **32**(1978) 583–591; *MR* **58** #10711.

D3. 图 形 数

Mordell 在他的书 p. 259 上问道:是否方程

$$6y^2 = (x+1)(x^2-x+6)$$

的仅有的整数解由 $x = -1,0,2,7,15$ 和 74 给出? 根据 Mordell 的书中第 27 章的定理 1,它只有有限多个解. 该方程是从

$$y^2 = \binom{x}{0} + \binom{x}{1} + \binom{x}{2} + \binom{x}{3}$$

提出来的. Andrew Bremner 给出了另外的解 $(x,y) = (767, 8672)$,并证明了这些就是全部的解,不过这个结果已在 1971 年由 Ljunggren 给出.

类似地，Martin Gardner 取图形数：三角数，平方数，四面体数以及正方金字塔数. 把它们对列成方程式. 在得到的六个问题中，他注意到除了"三角数 = 正方金字塔数"这个问题外，其余问题全都得到了解决. 由"三角数 = 正方金字塔数"这个问题引导出方程

$$3(2y+1)^2 = 8x^3 + 12x^2 + 4x + 3,$$

其解数仍是有限的. 所有的解是否是由 $x = -1, 0, 1, 5, 6$ 和 85 给出呢? Schinzel 给出了 Avanesov 对此问题的肯定的回答，而 Uchiyama 又重新发现了这一结果.

"三角数 = 四面体数"问题是有关二项系数的等式的一个特例(见 B31).

$$\binom{n}{2} = \binom{m}{3}$$

的仅有的非平凡的例子是 $(m, n) = (10, 16), (22, 56)$ 和 $(36, 120)$.

$$\binom{n}{2} = \binom{m}{4}$$

有除了(10,21)以外的非平凡的例子吗?

"正方金字塔数 = 平方数"是 Lucas 的问题. $x = 24, y = 70$ 是不定方程

$$y^2 = x(x+1)(2x+1)/6$$

的惟一的非平凡解吗? 这由 Watson 用椭圆函数给予肯定的回答，也由 Ljunggren 用二次域中的 Pell 方程获得解决. Mordell 问是否有一个初等证明? Ma De-Gang，Xu Z. Y 和曹珍富(Cao Zhen-Fu)，Anglin 以及 Pintér 等人对此给出了肯定的回答.

由于上面的方程可以写成

$$(2y)^2 = 2x(2x+1)(2x+2)/6,$$

经变形后的同样的方程要问的问题是：(48,140)是否是"平方数 = 四面体数"情形惟一的非平凡解? 尽管如 Peter Montgomery 所注意到的，这里并不排除奇数平方的可能性. 更为现代的一种处理方法是令 $12x = X - 6$, $72y = Y$，并注意 $Y^2 = X^3 - 36X$ 是 John

Cremona 的表中的曲线 576H2. 点(12,36)(它给出一个奇数的平方)作为生成元. 它有无穷多个有理解,但仅有原问题的非平凡的整数解是由点(294,5040)给出的.

比"寻求前 n 个平方数的和是一个平方数"更为一般的问题是:寻求 n 个连续的平方数,使其和是一个平方数. 如果 S 是使之能成立的 n 之集合,那么已知 S 是无限的,但其密度为零,且如果 n 是 S 的一个非平方数的元素,那么对这样的 n 有无穷多个解. 如果 $N(x)$ 表示 S 中小于 x 的元素个数,那么已知最好的结果是

$$c\sqrt{x} < N(x) = O\left(\frac{x}{\ln x}\right).$$

当 $1<n<73$ 时,S 中的元素以及使得从 a 开始的 n 个平方数的和是一个平方数的那种 a 的相应的最小值是

n	2	11	23	24	26	33	47	49	50	59
a	3	18	7	1	25	7	539	25	7	22.

更一般地,还可以要求一个任意的算术级数的元素的平方和是一个平方和. K. R. S. Sastry 注意到,如果该级数的项的个数是平方数,则此情形有可能发生.

为回答下述问题:什么样的三角数是三个相连整数之积? Tzanakis 和 de Weger 给出了(仅有的)答案:6,120,210,990,185136 和 258474216. 遗憾的是,Mohanty 对同一结果所作的初等证明是错的.

椭圆曲线的其他例子由 Bremner 和 Tzanakis 作了处理,他们证明了:$y^2 = x^3 - 7x + 10$ 恰有 26 个整点,他们还对 $(b,c) = (172,505)$,$(172,820)$和$(112,2320)$检查了曲线 $y^2 = x^3 - bx + c$.

对 $k=3$,$\binom{a}{k} - \binom{b}{k} = c^k$ 有无穷多个解. 对 $k=4$ 它有解吗? 对 $k=5$,$(a,b,c)=(18,12,6)$是一个孤立的例子吗?

参考文献

H. L. Abbott, P. Erdős & D. Hanson, On the number of times an integer occurs as a binomial coefficient, *Amer. Math. Monthly*, **81**(1974) 256–261.

S. C. Althoen & C. Lacampagne, Tetrahedral numbers as sums of square numbers, *Math. Mag.*, **64**(1991) 104–108.

W. S. Anglin, The square pyramid puzzle, *Amer. Math. Monthly*, **97**(1990) 120–124; *MR* **91e**:11026.

È. T. Avanesov, The Diophantine equation $3y(y+1) = x(x+1)(2x+1)$ (Russian), *Volž. Mat. Sb. Vyp.*, **8**(1971) 3–6; *MR* **46** #8967.

È. T. Avanesov, Solution of a problem on figurate numbers (Russian), *Acta Arith.*, **12**(1966/67) 409–420; *MR* **35** #6619.

E. Barbette, Les sommes de p-ièmes puissances distinctes égales à une p-ième puissance, Liège, 1910, 77–104.

Laurent Beeckmans, Squares expressible as the sum of consecutive squares, *Amer. Math. Monthly*, **100**(1993)

Andrew Bremner, An equation of Mordell, *Math. Comput.*, **29**(1975) 925–928; *MR* **51** #10219.

Andrew Bremner & Nicholas Tzanakis, Integer points on $y^2 = x^3 - 7x + 10$, *Math. Comput.*, **41**(1983) 731–741.

J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1992. [Information for conductor 702, inadvertently omitted from the tables, is obtainable from the author.]

Ion Cucurezeanu, An elementary solution of Lucas' problem, *J. Number Theory*, **44**(1993) 9-12.

H. E. Dudeney, *Amusements in Mathematics*, Nelson, 1917, 26, 167.

P. Erdős, On a Diophantine equation, *J. London Math. Soc.*, **26**(1951) 176–178; *MR* **12**, 804d.

Raphael Finkelstein, On a Diophantine equation with no non-trivial integral solution, *Amer. Math. Monthly*, **73**(1966) 471–477; *MR* **33** #4004.

Martin Gardner, Mathematical games, On the patterns and the unusual properties of figurate numbers, *Sci. Amer.*, **231** No. 1 (July, 1974) 116–120.

Charles M. Grinstead, On a method of solving a class of Diophantine equations, *Math. Comput.*, **32**(1978) 936–940; *MR* **58** #10724.

Heiko Harborth, Fermat-like binomial equations, in Applications of Fibonacci Numbers, Kluwer, 1988, 1–5.

Moshe Laub, O. P. Lossers & L. E. Mattics, Problem 6552 and solution, *Amer. Math. Monthly*, **97**(1990) 622–625.

D. A. Lind, The quadratic field $Q(\sqrt{5})$ and a certain Diophantine equation, *Fibonacci Quart.*, **6**(1968) 86–93.

W. Ljunggren, New solution of a problem proposed by E. Lucas, *Norsk Mat. Tidskr.*, **34**(1952) 65–72; *MR* **14**, 353h.

W. Ljunggren, A diophantine problem, *J. London Math. Soc.* (2), **3**(1971) 385–391; *MR* **45** #171.

E. Lucas, Problem 1180, *Nouv. Ann. Math.*(2), **14**(1875) 336.

Ma De-Gang, An elementary proof of the solution to the Diophantine equation $6y^2 = x(x+1)(2x+1)$, *Sichuan Daxue Xuebao*, 4(1985) 107–116; *MR* **87e**:11039.

S. P. Mohanty, Integer points of $y^2 = x^3 - 4x + 1$, *J. Number Theory*, **30**(1988) 86-93; *MR* **90e**:11041a; but see A. Bremner, **31**(1989) 373; **90e**:11041b.

Ákos Pintér, A new solution of two old diophantine equations, Technical Report No. 92 (1993), Department of Mathematics, Kossuth University, Debrecen, Hungary.

David Singmaster, How often does an integer occur as a binomial coefficient? *Amer. Math. Monthly*, **78**(1971) 385–386.

David Singmaster, Repeated binomial coefficients and Fibonacci numbers, *Fibonacci Quart.*, **13** (1975) 295–298.

Craig A. Tovey, Multiple occurrences of binomial coefficients, *Fibonacci Quart.*, **23**(1985) 356–358.

N. Tzanakis & B. M. M. de Weger, On the practical solution of the Thue equation, *J. Number Theory*, **31**(1989) 99-132; *MR* **90c**:11018.

Saburô Uchiyama, Solution of a Diophantine problem, *Tsukuba J. Math.*, **8**(1984) 131–137; *MR* **86i**:11010.

G. N. Watson, The problem of the square pyramid, *Messenger of Math.*, **48** (1918/19) 1–22.

Z. Y. Xu & Cao Zhen-Fu, On a problem of Mordell, *Kexue Tongbao*, **30**(1985) 558–559.

D4. l 个 k 次幂的和

令 $r_{k,l}(n)$ 为 $n = \sum_{i=1}^{l} x_i^k$ 的正整数解 $\{x_i\}$ 的个数. Hardy 和 Littlewood 的猜想 K 是说:对 $\varepsilon>0$ 有 $r_{k,k}(n)=O(n^{\varepsilon})$. 对 $k=2$ 这是熟知的结果.事实上,对充分大的 n 有

$$r_{2,2}(n) < n(1+\varepsilon)\ln 2/\ln\ln n,$$

此外,如果用另外的更小的数代替 ln 2,则结论不再成立. Mahler 指出:对无穷多个 n 有 $r_{3,3}(n)>c_1 n^{1/12}$,从而推翻了 $k=3$ 时的猜想.

Erdös 认为有可能对所有 n 有 $r_{3,3}(n)<c_2 n^{1/12}$,但现在对此还一无所知. 可能猜想 K 对每个 $k\geqslant 3$ 都是错的,然而也可能对充分大的 x 有 $\sum_{n=1}^{x}(r_{k,k}(n))^2 < x^{1+\varepsilon}$.

S. Chowla 证明了对 $k\geqslant 5$ 有 $r_{k,k}(n)\neq O(1)$,他还和 Erdös

一起证明了，对每个 $k\geqslant 2$ 和无穷多个 n 有

$$r_{k,k}(n) > \exp(c_k \ln n / \ln\ln n).$$

Mordell 证明了 $r_{3,2}(n)\neq O(1)$，Mahler 证明了对无穷多个 n 有 $r_{3,2}(n)>(\ln n)^{1/4}$. 对 $r_{3,2}(n)$ 还不知道有非平凡的上界. Jean Lagrange 证明了 $\limsup r_{4,2}(n)\geqslant 2$ 以及 $\limsup r_{4,3}(n)=\infty$.

另一个棘手的问题是估计可以表为 l 个 k 次幂之和的数 $n\leqslant x$ 的个数 $A_{k,l}(x)$. Landau 证明了

$$A_{2,2}(x) = (c+o(1))x/(\ln x)^{1/2},$$

Erdös 和 Mahler 证明了，如果 $k>2$，则有 $A_{k,2}>c_k x^{2/k}$，Hooley 证明了 $A_{k,2}>(c_k+o(1))x^{2/k}$. 似乎肯定有：若 $l<k$，则有 $A_{k,l}>c_{k,l}x^{l/k}$，又对每个 ϵ 有 $A_{k,k}>x^{1-\epsilon}$，但这些结果都还没有得到证明.

从 Chowla-Erdös 的结果可以推出：对所有 k 存在一个 n_k，使 $n_k=p^3+q^3+r^3$ 的解数大于 k. 对多于 3 个加数的情形，目前尚不知道相对应的结果.

参考文献

S. Chowla, The number of representations of a large number as a sum of non-negative nth powers, *Indian Phys.-Math. J.*, **6**(1935) 65–68; *Zbl.* **12**.339.

H. Davenport, Sums of three positive cubes, *J. London Math. Soc.*, **25**(1950) 339–343; *MR* **12**, 393.

P. Erdős, On the representation of an integer as the sum of k kth powers, *J. London Math. Soc.*, **11**(1936) 133–136; *Zbl.* **13**.390.

P. Erdős, On the sum and difference of squares of primes, I, II, *J. London Math. Soc.*, **12**(1937) 133–136, 168–171; *Zbl.* **16**.201, **17**.103.

P. Erdős & K. Mahler, On the number of integers that can be represented by a binary form, *J. London Math. Soc.*, **13**(1938) 134–139; *Zbl.* **13**.390.

P. Erdős & E. Szemerédi, On the number of solutions of $m=\sum_{i=1}^{k} x_i^k$, *Proc. Symp. Pure Math.*, **24** Amer. Math. Soc., Providence, 1972, 83–90.

W. Gorzkowski, On the equation $x_0^2+x_1^2+\ldots+x_n^2=x_{n+1}^k$, *Ann. Soc. Math. Polon. Ser. I Comment. Math. Prace Mat.*, **10**(1966) 75–79; *MR* **32** #7495.

G. H. Hardy & J. E. Littlewood, Partitio Numerorum VI: Further researches in Waring's problem, *Math. Z.*, **23**(1925) 1–37.

Jean Lagrange, Thèse d'État de l'Université de Reims, 1976.
K. Mahler, On the lattice points on curves of genus 1, *Proc. London Math. Soc.*, **39**(1935) 431–466.
K. Mahler, Note on Hypothesis K of Hardy and Littlewood, *J. London Math. Soc.*, **11**(1936) 136–138.

D5. 4个立方和

每个数都是4个立方和吗？除了对形如 $9n \pm 4$ 的数尚不知结论是否成立外，对所有其他的数，这一结论都已得到证明.

更进一步要问：是否每个数都是其中有两个数相等的4个立方数之和？特别地，方程 $76 = x^3 + y^3 + 2z^3$ 有解吗？在小于1000的数中，剩下的仍有怀疑的数是148，183，230，356，418，428，445，482，491，580，671，788，931和967. 在M. Lal于1970年1月20日写给A. Mąkowski的一封信中提及J. C. Littlejohn的如下的发现：$253 = 0^3 + 5^3 + 2 \cdot 4^3$，$519 = 0^3 + 17^3 + 2 \cdot (-13)^3$，$734 = (-520)^3 + (-700)^3 + 2 \cdot 623^3$. Andrew Bremner告诉我有 $923 = 27512^3 + (-27517)^3 + 2 \cdot 1784^3$.

所有不是形如 $9n \pm 4$ 的数都是三个立方之和吗？对所有小于1000的数用计算机搜索后发现：除了数

30	33	42	52	74	75	84	110	114
156	165	195	290	318	366	390	420	435
444	452	462	478	501	530	534	564	579
588	600	606	609	618	627	633	732	735
758	767	786	789	795	830	834	861	894
903	906	912	921	933	948	964	969	975

以外，对其他的数都找到了这样的表示. 在1993年5月25日的一封电子邮件中，Andrew Bremner告诉我有

$$75 = 435203083^3 + (-435203231)^3 + 4381159^3$$

（它给出600的一个非本原的解），而Conn和Vaserstein则发现了

$$84 = 41639611^3 + (-41531726)^3 + (-8241191)^3.$$

方程 $3 = x^3 + y^3 + z^3$ 有解(1,1,1)和(4,4,-5). 它还有其他的解吗?

参考文献

J. W. S. Cassels, A note on the Diophantine equation $x^3 + y^3 + z^3 = 3$, *Math. Comput.*, **44**(1985) 265–266; *MR* **86d**:11021.

W. Conn & L. N. Vaserstein, On sums of three integral cubes, *Contemporary Math.*, (to appear).

S. W. Dolan, On expressing numbers as the sum of two cubes, *Math. Gaz.*, **66**(1982) 31–38.

W. J. Ellison, Waring's problem, *Amer. Math. Monthly*, **78**(1971) 10–36.

V. L. Gardiner, R. B. Lazarus & P. R. Stein, Solutions of the diophantine equation $x^3 + y^3 = z^3 - d$, *Math. Comput.*, **18**(1964) 408–413; *MR* **31** #119.

D. R. Heath-Brown, W. M. Lioen & H. J. J. te Riele, On solving the Diophantine equation $x^3 + y^3 + z^3 = k$ on a vector computer, *Math. Comput.*, **61**(1993) 235–244.

Chao Ko, Decompositions into four cubes, *J. London Math. Soc.*, **11**(1936) 218–219.

Kenyi Koyama, On the solutions of the Diophantine equation $x^3 + y^3 + z^3 = n$ (preprint).

M. Lal, W. Russell & W. J. Blundon, A note on sums of four cubes, *Math. Comput.*, **23**(1969) 423–424; *MR* **39** #6819.

A. Mąkowski, Sur quelques problèmes concernant les sommes de quatre cubes, *Acta Arith.*, **5**(1959) 121–123; *MR* **21** #5609.

J. C. P. Miller & M. F. C. Woollett, Solutions of the diophantine equation $x^3 + y^3 + z^3 = k$, *J. London Math. Soc.*, **30**(1955) 101–110; *MR* **16**, 797e.

W. Scarowsky & A. Boyarsky, A note on the Diophantine equation $x^n + y^n + z^n = 3$, *Math. Comput.*, **42**(1984) 235–237; *MR* **85c**:11029.

A. Schinzel & W. Sierpiński, Sur les sommes de quatre cubes, *Acta Arith.*, **4**(1958) 20–30.

Sun Qi, On Diophantine equation $x^3 + y^3 + z^3 = n$, *Kexue Tongbao*, **33**(1988) 2007–2010; *MR* **90g**:11033 (see also **32**(1987) 1285–1287).

D6. $x^2 = 2y^4 - 1$ 的一个初等解法

Ljunggren 证明了 $y^2 = 2x^4 - 1$ 仅有的正整数解是(1,1)和(239,13),但他的证明很艰深. Mordell 问是否能找到一个简单而初等的证明? Whether Steiner 和 Tzanakis 简化了这一解法,或许

别有一番风味：他们用到代数数对数的线性型的理论.

Ljunggren 和其他人对类似的方程作了许多研究. 有关参考文献见本书第一版. Cohn 对所有 $D \leqslant 400$ 考虑了方程 $y^2 = Dx^4 + 1$. 恰好当在曲线 $y^2 = x(x^2 - 4D)$ 和 $Y^2 = X(X^2 + 16D)$ 上(只要 $\pm D$ 不是平方数，它们就是非奇异的)有有理点时，它有有理解.

参考文献

J. H. E. Cohn, The diophantine equation $y^2 = Dx^4 + 1$, I, *J. London Math. Soc.*, **42**(1967) 475–476; *MR* **35** #4158; II, *Acta Arith.*, **28**(1975/76) 273–275; *MR* **52** #8029; III, *Math. Scand.*, **42**(1978) 180–188; *MR* **80a**:10031.

W. Ljunggren, Some remarks on the diophantine equations $x^2 - \mathcal{D}y^4 = 1$ and $x^4 - \mathcal{D}y^2 = 1$, *J. London Math. Soc.*, **41**(1966) 542–544; *MR* **33** #5555.

L. J. Mordell, The diophantine equation $y^2 = Dx^4 + 1$, *J. London Math. Soc.*, **39**(1964) 161–164; *MR* **29** #65.

Ray Steiner & Nikos Tzanakis, Simplifying the solution of Ljunggren's equation $X^2 + 1 = 2Y^4$, *J. Number Theory*, **37**(1991) 123–132; *MR* **91m**:11018.

D7. 相邻幂和做成的幂

Rufus Bowen 猜想：方程

$$1^n + 2^n + \cdots + m^n = (m+1)^n$$

没有非平凡的解，而 Leo Moser 证明了：对 $m \leqslant 10^{1000000}$ 它没有非平凡的解，对奇数 n 也没有非平凡的解. Zhou Guo-Fu 和 Kang Ji-Ding 将这个界提高到 $m \leqslant 10^{2000000}$. Van de Lune 和 te Riele 证明了，该方程几乎永不可解. 注意 $n \sim m \ln 2$.

Tijdeman 注意到，有关方程

$$1^n + 2^n + \cdots + k^n = m^n$$

的一般性的结果与这一特殊方程好像没有什么关系.

Erdös 提出如下问题：如果 m, n 是满足(K)的整数，试证明(L′)和(M′)为真，这里

(K) $\quad \left(1 - \frac{1}{m}\right)^n > \frac{1}{2} > \left(1 - \frac{1}{m-1}\right)^n$,

(L′) $\quad 1^n + 2^n + \cdots + (m-2)^n < (m-1)^n$,

$$(\mathrm{M}') \quad 1^n + 2^n + \cdots + m^n > (m+1)^n,$$

且(L)和(M)均无穷多次为真,这里

$$(\mathrm{L}) \quad 1^n + 2^n + \cdots + (m-1)^n < m^n,$$

$$(\mathrm{M}) \quad 1^n + 2^n + \cdots + (m-1)^n > m^n.$$

Van de Lune 证明了(K)蕴含(L′),Best 和 te Riele 证明了(K)蕴含(M′),且(M)对 $m \leqslant x$ 中至多 $c\ln x$ 个值成立. Van de Lune 和 te Riele 证明了(L)对几乎所有的数对(m,n)为真. Best 和 te Riele 计算了使(K)和(M)两者都成立的 33 对(m,n),其中最小的一对是

$$m = 1121626023352385, \quad n = 777451915729368.$$

有无穷多个这样的数对吗?

最近,Pieter Moree, te Riele 和 Urbanowicz 证明了:在原方程中 n 必须被直到 200 的所有整数的最小公倍数整除,而 m 既不被任何正则素数整除(见 D2),也不被任何<1000 的非正则素数整除.

参考文献

M. R. Best & H. J. J. te Riele, On a conjecture of Erdős concerning sums of powers of integers, *Report NW 23/76*, Mathematisch Centrum Amsterdam, 1976.

P. Erdős, Advanced problem 4347, *Amer. Math. Monthly*, **56**(1949) 343.

K. Györy, R. Tijdeman & M. Voorhoeve, On the equation $1^k + 2^k + \cdots + x^k = y^z$, *Acta Arith.*, **37**(1980) 233–240.

J. van de Lune, On a conjecture of Erdős (I), *Report ZW 54/75*, Mathematisch Centrum Amsterdam, 1975.

J. van de Lune & H. J. J. te Riele, On a conjecture of Erdős (II), *Report ZW 56/75*, Mathematisch Centrum Amsterdam, 1975.

J. van de Lune & H. J. J. te Riele, A note on the solvability of the diophantine equation $1^n + 2^n + \cdots + m^n = G(m+1)^n$, *Report ZW 59/75*, Mathematisch Centrum Amsterdam, 1975.

P. Moree, H. J. J. te Riele & J. Urbanowicz, Divisibility properties of integers x and k satisfying $1^k + 2^k + \cdots + (x-1)^k = x^k$, *Math. Comput.*, **62**(1994).

L. Moser, On the diophantine equation $1^n + 2^n + \cdots + (m-1)^n = m^n$, *Scripta Math.*, **19**(1953) 84–88; *MR* **14**, 950.

J. J. Schäffer, The equation $1^p + 2^p + \cdots + n^p = m^q$, *Acta Math.*, **95**(1956) 155–189; *MR* **17**, 1187.

Jerzy Urbanowicz, Remarks on the equation $1^k+2^k+\cdots+(x-1)^k=x^k$, *Nederl. Akad. Wetensch. Indag. Math.*, **50**(1988) 343–348; *MR* **90b**:11026.
M. Voorhoeve, K. Györy & R. Tijdeman, On the diophantine equation $1^k+2^k+\cdots+x^k+R(x)=y^z$, *Acta Math.*, **143**(1979) 1–8; *MR* **80e**:10020.
Zhou Guo-Fu & Kang Ji-Ding, On the diophantine equation $\sum_{k=1}^{m} k^n=(m+1)^n$, *J. Math. Res. Exposition*, **3**(1983) 47–48; *MR* **85m**:11020.

D8. 棱锥型不定方程

Wunderlich 要求方程 $x^3+y^3+z^3=x+y+z$ 的所有解(的参数表示). Bernstein, S. Chowla, Edgar, Fraenkel, Oppenheim, Segal 以及 Sierpiński 给出了它的解,其中有一些是参数解,因此它确有无穷多个解. 它们中的 88 个有少于 13000 个未知数. Bremner 有效地确定了它所有的参数解.

参考文献

Leon Bernstein, Explicit solutions of pyramidal Diophantine equations, *Canad. Math. Bull.*, **15**(1972) 177–184; *MR* **46** #3442.
Andrew Bremner, Integer points on a special cubic surface, *Duke Math. J.*, **44**(1977) 757-765; *MR* **58** #27745.
Hugh Maxwell Edgar, Some remarks on the Diophantine equation $x^3+y^3+z^3=x+y+z$, *Proc. Amer. Math. Soc.*, **16**(1965) 148–153; *MR* **30** #1094.
A. S. Fraenkel, Diophantine equations involving generalized triangular and tetrahedral numbers, in *Computers in Number Theory, Proc. Atlas Symp. No. 2*, Oxford, 1969, Academic Press, 1971, 99–114; *MR* **48** #231.
A. Oppenheim, On the Diophantine equation $x^3+y^3+z^3=x+y+z$, *Proc. Amer. Math. Soc.*, **17**(1966) 493–496; *MR* **32** #5590.
A. Oppenheim, On the diophantine equation $x^3+y^3+z^3=px+py-qz$, *Univ. Beograd Publ. Elektrotehn. Fac. Ser.* #235(1968); *MR* **39** #126.
S. L. Segal, A note on pyramidal numbers, *Amer. Math. Monthly*, **69**(1962) 637–638; *Zbl.* **105**, 36.
W. Sierpiński, Sur une propriété des nombres tétraédraux, *Elem. Math.*, **17**(1962) 29–30; *MR* **24** #A3118.
W. Sierpiński, Trois nombres tétraédraux en progression arithmetique, *Elem. Math.*, **18**(1963) 54–55; *MR* **26** #4957.
M. Wunderlich, Certain properties of pyramidal and figurate numbers, *Math. Comput.*, **16**(1962) 482–486; *MR* **26** #6115.

D9. 两个幂之差

除了还剩下有限的计算量之外,Tijdeman 解决了 Catalan 的古老的猜想:高于一次的仅有的相差为 1 的幂是 2^3 和 3^2. 但是这里说的有限的计算量仍然超出了计算机的能力范围,如果没有理论上的某些额外的新思想,这些计算是不可能完成的. Langevin 从 Tijdeman 的证明推出:如果 n 和 $n+1$ 是两个幂,则 $n<\exp\exp\exp\exp 730$. Aaltonen 和 Inkeri 证明了:$x^p-y^q=1$ 和 $x,y>2$ 蕴含 $x,y>10^{500}$. Mignotte 证明了:$p<1.21\times10^{26}$, $q<1.31\times10^{18}$. 如果 p 和 q 都是素数,且 $q\equiv 3 \bmod 4$,那么这些界可以被减小到 2.7×10^{24} 和 1.23×10^{18}. 如果 $\min\{p,q\}=2$ 或 3,则没有解. Glass 和其他人对 $\min\{p,q\}\in\{5,7,11\}$ 证明了此结论仍然为真. Mignotte 指出:对 $p=19$ 它无解,而对 $p=53$ 惟一有解的可能是 $q=4889$.

Bennett 证明了:如果 $4\leqslant N\leqslant k\cdot 3^k$,则有

$$\left\|\left(\frac{N+1}{N}\right)^k\right\|>3^{-k},$$

这里 $\|x\|$ 是 x 离最近整数的距离.

Leech 问:$|a^m-b^n|<|a-b|$ 是否有满足 $m,n\geqslant 3$ 的解? 关于等式,他注意到有 $|5^3-2^7|=5-2$ 和 $|13^3-3^7|=13-3$. 这些是否是全部的解? 上面等式中的幂 3 和 7 有何意义?

如果 $a_1=4, a_2=8, a_3=9,\cdots$ 是高于 1 的幂的序列,Chudnowsky 宣布他证明了 $a_{n+1}-a_n$ 与 n 一起趋向无穷. Erdös 猜想有 $a_{n+1}-a_n>c'n^c$,但是他说现在没有希望证明这一猜想.

Erdös 问:是否存在无穷多个不是形如 x^k-y^l 的数($k>1$, $l>1$)?

Carl Rudnick 用 $N(r)$ 记 $x^4-y^4=r$ 的正的解的个数,并问 $N(r)$ 是否有界? Hansraj Gupta 注意到,Hardy 和 Wright(p.201)

用 Swinnerton-Dyer 的表述形式给出了方程 $x^4 - y^4 = u^4 - v^4$ 的 Euler 的参数解，这一结果说明 $N(r)$ 无穷多次取值 0,1 或 2. 例如 $133^4 - 59^4 = 158^4 - 134^4 = 300783360$. 作为 $N(r) = 3$ 的一个例子，Zajta 给出

$$401168^4 - 17228^4 = 415137^4 - 248289^4 = 421296^4 - 273588^4.$$

对 $N(r)$ 有界这一点几乎没有什么怀疑.

Hugh Edgar 问：对素数 p 和 q 以及整数 h, $p^m - q^n = 2^h$ 有多少个解 (m,n)？解的例子有 $3^2 - 2^3 = 2^0$, $3^3 - 5^2 = 2^1$, $5^3 - 11^2 = 2^2$, $5^2 - 3^2 = 2^4$, $3^4 - 7^2 = 2^5$. 还有其他的解吗？Andrzej Schinzel 写道：Gelfond 以及 Rumsey 和 Posner 的工作说明该方程仅有有限多个解. Reese Scott 为解决此问题走了相当长的路. 他注意到，对给定的 $(p, q, c(=2^h))$，从 Pillai 的一个结果可以推导出解数有限，并证明了此解数常常至多是 1（除了少数特别列出的例外情形），而在那些例外的情形，解数或者是 2，或者可能是 3.

参 考 文 献

M. Aaltonen & K. Inkeri, Catalan's equation $x^p - y^q = 1$ and related congruences, *Math. Comput.*, **56**(1991) 359–370; *MR* **91g**:11025.

David M. Battany, Advanced Problem 6110*, *Amer. Math. Monthly*, **83** (1976) 661.

M. Bennett, Fractional parts of powers of rational numbers, *Math. Proc. Cambridge Philos. Soc.*, **114**(1993) 191–201.

Cao Zhen-Fu, Hugh Edgar's problem on exponential Diophantine equations (Chinese), *J. Math. (Wuhan)*, **9**(1989) 173–178; *MR* **90i**:11035.

Cao Zhen-Fu & Wang Du-Zheng, On the Diophantine equation $a^x - b^y = (2p)^z$ (Chinese). *Yangzhou Shiyuan Xuebao Ziran Kexue Ban*, **1987** no. 4 25–30; *MR* **90c**:11020.

P. S. Dyer, A solution of $A^4 + B^4 = C^4 + D^4$, *J. London Math. Soc.*, **18**(1943) 2–4; *MR* **5**, 89e.

A. O. Gelfond, Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un idéal premier, *Mat. Sbornik*, **7**(1940) 724.

A. M. W. Glass, D. B. Meronk, T. Okada & R. P. Steiner, A small contribution to Catalan's equation, 1992 (to appear).

Aaron Herschfeld, The equation $2^x - 3^y = d$, *Bull. Amer. Math. Soc.*, **42** (1936) 231-234; *Zbl.* **14** 8a.

K. Inkeri, On Catalan's conjecture, *J. Number Theory*, **34** (1990) 142–152; *MR* **91e**:11030.

Michel Langevin, Quelques applications de nouveaux résultats de Van der Poorten, *Sém. Delange-Pisot-Poitou*, (1975/76). *Théorie des nombres: Fasc.* 2, *Exp. No.* G12, Paris, 1977; *MR* **58** #16550.
Le Mao-Hua, A note on the diophantine equation $ax^m - by^n = k$, *Indag. Math.* (*N.S.*), **3**(1992) 185–191; *MR* **93c**:11016.
Maurice Mignotte, Sur l'équation de Catalan, *C.R. Acad. Sci. Paris Sér. I Math.*, **314**(1992) 165–168; *MR* **93e**:11044.
M. Mignotte, Sur l'équation de Catalan, II, *Theor. Comput. Sci.*, **123**(1994) 145–149.
Trygve Nagell, Sur une classe d'équations exponentielles, *Ark. Mat.*, **3**(1958) 569–582; *MR* **21** #2621.
S. Sivasankaranarayana Pillai, On the inequality "$0 < a^x - b^y \le n$", *J. Indian Math. Soc.*, **19**(1931) 1–11; Zbl. **1** 268b.
S. S. Pillai, On $a^x - b^y = c$, *ibid.* (N.S.) **2**(1936) 119–122; Zbl. **14** 392e.
S. S. Pillai, A correction to the paper "On $A^x - B^y = C$", *ibid.* (N.S.) **2**(1937) 215; Zbl. **16** 348b.
Howard Rumsey & Edward C. Posner, On a class of exponential equations, *Proc. Amer. Math. Soc.*, **15**(1964) 974–978.
Reese Scott, On the equations $p^x - b^y = c$ and $a^x + b^y = c^z$, *J. Number Theory*, **44**(1993) 153–165.
R. Tijdeman, On the equation of Catalan, *Acta Arith.*, **29**(1976) 197–209; *MR* **53** #7941.
Aurel J. Zajta, Solutions of the Diophantine equation $A^4 + B^4 = C^4 + D^4$, *Math. Comput.*, **41**(1983) 635–659, esp. p. 652; *MR* **85d**:11025.

D10. 指数型不定方程

Bremner 和 Foster 提出了下面的一般性的问题：令 $\{p_i\}$ 是一个有限的素数集，$\varepsilon = \pm 1$，什么时候指数型不定方程 $\sum \varepsilon_i p_i^{x_i} = 0$ 能用初等方法(例如模算术)求解？更确切地说，给定 p_i，ε_i，什么样的判别法能确定：是否存在一个模 M，使给定的方程等价于同余式 $\sum \varepsilon_i p_i^{x_i} \equiv 0 \bmod M$？他们解决了许多特殊的情形，在大多数情形，$p_i$ 的个数为 4，但是小于 108. 在某些情形(甚至在有两个素数相等的时候)初等方法有用，但在一般的情形，初等方法不起作用. 事实上，不论是 $3^a = 1 + 2^b + 2^c$ 还是 $2^a + 3^b = 2^c + 3^d$ 都不能化为单个的同余式. Tijdeman 注意到，解这些纯指数型不定方程(它们在群论中有一定的作用)的另一种方法是 Baker 的方法(与 F23 比较). 这使得有可能去求解最后那两个方程.

Hugh Edgar 问：方程 $1+q+q^2+\cdots+q^{x-1}=p^y$（$p,q$ 为奇素数，$x\geqslant5,y\geqslant2$）除了解 $1+3+3^2+3^3+3^4=11^2$ 以外还有别的解吗？在这方面一个重要的突破是 Reese Scott 的论文（见 D9）.

参考文献

Leo J. Alex, Problem E2880, *Amer. Math. Monthly*, **88**(1981) 291.

Leo J. Alex, Problem 6411, *Amer. Math. Monthly*, **89**(1982) 788.

Leo J. Alex, The diophantine equation $3^a+5^b=7^c+11^d$, *Math. Student*, **48**(1980) 134–138 (1984); *MR* **86e**:11022.

Leo J. Alex & Lorraine L. Foster, Exponential Diophantine equations, in *Théorie des nombres, Québec 1987*, de Gruyter, Berlin – New York (1989) 1–6; *MR* **90d**:11030.

J. L. Brenner & Lorraine L. Foster, Exponential Diophantine equations, *Pacific J. Math.*, **101**(1982) 263–301; *MR* **83k**:10035.

Lorraine L. Foster, Solution to Problem S31 [1980, 403], *Amer. Math. Monthly*, **89**(1982) 62.

Guo Zhi-Tang & Wu Yun-Fei, On the equation $1+q+q^2+\cdots+q^{n-1}=p^m$ (Chinese), *J. Harbin Inst. Tech.*, **24**(1992) 6–9; *MR* **93k**:11024.

Le Mao-Hua, A note on the Diophantine equation $(x^m-1)/(x-1)=y^n$, *Acta Arith.*, **64**(1993) 19–28.

A. Mąkowski & A. Schinzel, Sur l'équation indéterminée de R. Goormachtigh, *Mathesis*, **68**(1959) 128–142; *MR* **22** #9472.

Mo De-Ze & R. Tijdeman, Exponential Diophantine equations with four terms, *Indag. Math.(N.S.)*, **3**(1992) 47–57; *MR* **93d**:11035.

A. Rotkiewicz & W. Złotkowski, On the Diophantine equation $1+p^{\alpha_1}+p^{\alpha_2}+\ldots+p^{\alpha_k}=y^2$, in Number Theory, Vol. II (Budapest, 1987), North-Holland, *Colloq. Math. Soc. János Bolyai*, **51**(1990) 917–937; *MR* **91e**:11032.

T. N. Shorey, Integers with identical digits, *Acta Arith.*, **53** (1989) 187–205; *MR* **90j**:11027.

Christopher M. Skinner, On the Diophantine equation $ap^x+bq^y=c+dp^zq^w$, *J. Number Theory*, **35**(1990) 194–207; *MR* **91h**:11021.

Robert Styer, Small two-variable exponential Diophantine equations, *Math. Comput.*, **60**(1993) 811–816.

B. M. M. de Weger, Solving exponential Diophantine equations using lattice basis reduction algorithms, *J. Number Theory*, **26**(1987) 325–367; erratum **31**(1989) 88-89; *MR* **88k**:11097 **90a**:11040.

D11. 埃及分数

Rhind 纸草纸是流传至今最古老的用文字记载的数学之一，

它讨论的是有理数表示成单位分数之和的问题

$$\frac{m}{n}=\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_k}.$$

它引出大量的问题,其中许多问题尚未获得解决,它们还继续提出新的问题,于是对埃及分数的兴趣至今仍如以前一样强烈.文献显示只有一小部分内容被写了下来. Bleicher 对此写了一篇详尽的综述,它吸引人们注意对给定类型的表示法所构造出的各种算法:Fibonacci-Sylvester 算法,Erdös 算法,Golomb 算法和两个他自己的算法,Farey 级数算法以及连分数算法. 也见本卷书开始提到的 Erdös 和 Graham 的问题集中经过扩充的第四节以及可以从 Paul Campbell 的预印本中得到的文献.

Erdös 和 Straus 猜想:方程

$$\frac{4}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$$

对所有 $n>1$ 都有正整数解. 在 Mordell 的书中对此问题有很好的记述,在该书中证明了:除了 n 同余于 $1^2, 11^2, 13^2, 17^2, 19^2$ 和 $23^2 \bmod 840$ 之外,此猜想皆成立. 有若干人士研究过这个问题,其中包括 Bernstein, Obláth, Rosati, Shapiro, Straus, Yamamoto 以及 Nicola Franceschine. Nicola Franceschine 对 $n<10^8$ 验证了猜想. Schinzel 发现:仅当 b 不是 a 的二次剩余时($a \perp b$),可以用有正的首项系数的、t 的整多项式 $x(t), y(t), z(t)$ 来表示

$$\frac{4}{at+b}=\frac{1}{x(t)}+\frac{1}{y(t)}+\frac{1}{z(t)}.$$

Sierpiński 对

$$\frac{5}{n}=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}$$

做出了相应的猜想. Palamá 对所有 $n\leqslant 92231$ 证实了这一猜想, Stewart 将此扩大到 $n\leqslant 1057438801$,并对所有不是形如 $278460k+1$ 的 n 证明了猜想.

Schinzel 将要求 x, y, z 为正数这一条件放宽,并用一般的 m 代替分子 4 和 5,且只要求结论对 $n>n_m$ 成立. 由 $n_{18}=23$ 这个

例子表明，有可能 n_m 大于 m. 对 m 的连续大值，Schinzel, Sierpiński, Sedláček, Palamá 以及 Stewart 和 Webb 确立了猜想的正确性，Stewart 和 Webb 对 $m<36$ 给出了证明. Breusch 和 Stewart 相互独立地证明了：如果 $m/n>0$ 且 n 为奇数，那么 m/n 是有限多个奇整数的倒数之和. 也见 Graham 的论文. Vaughan 证明了：如果 $E_m(N)$ 是 $n\leqslant N$ 中使 $m/n=1/x+1/y+1/z$ 无解的整数之个数，那么

$$E_m(N)\ll N\exp\{-c(\ln N)^{2/3}\},$$

这里 c 只与 m 有关. Hofmeister 和 Stoll 证明了：如果 $F_m(N)$ 是 $n\leqslant N$ 中使 $m/n=1/x+1/y$ 无解的整数之个数，那么

$$F_m(N)\ll N(\ln N)^{-1/\varphi(m)},$$

其中 $\varphi(m)$ 是 Euler φ 函数(见 B36).

Hofmeister 注意到，这个结果蕴含 $A_m(N)/N\to1(N\to\infty)$, 其中 $A_m(N)$ 是 $1\leqslant b\leqslant N$ 中满足如下条件的整数 b 的个数：对这种 b 有一个表示 $m/b=1/n_1+1/n_2$，使得直线 $y=m(x\geqslant1)$ 上所有的格点都有一个这样的表示. 奇怪的是，Mittelbach 令 $B(N)$ 是 $1\leqslant a\leqslant b\leqslant N$ 中有一个表示 $a/b=1/n_1+1/n_2$ 的那种格点 (a,b) 的个数，他证明了有 $B(N)/\frac{1}{2}N(N+1)\to0$，也就是说，对很大的 N，在三角形 $(1,1),(1,N),(N,N)$ 内几乎没有格点能有这样的表示.

与 Breusch 和 Stewart 的结果形成对照的是，由 Stein, Selfridge, Graham 以及其他人所提出的下述问题仍未得到解决：如果一个有理数 m/n (n 是奇数)可以表为 $\sum 1/x_i$，这里 x_i 是连续选取的最小可能的奇整数，它使余项 $m/n-\sum 1/x_i$ 是一个非负的数，那么 m/n 是否总可以用一个有限的和来表示？例如

$$\frac{2}{7}=\frac{1}{5}+\frac{1}{13}+\frac{1}{115}+\frac{1}{10465}.$$

John Leech 在一封 1977 年 3 月 14 日写的信中问道：关于倒数之和为 1 的那种不相等的奇整数集，比如像

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{15}+\frac{1}{21}+\frac{1}{27}+\frac{1}{35}+\frac{1}{63}+\frac{1}{105}+\frac{1}{135}=1,$$

我们知道些什么呢？他说，一个这样的集合至少需要 9 个奇数，另一方面，其中最大的分母必须至少是 105. 注意它和 Sierpiński 的伪完全数(B2)之间的联系.

$945 = 315 + 189 + 135 + 105 + 63 + 45 + 35 + 27 + 15 + 9 + 7.$

已知，如果 n 是奇数，那么 m/n 总可以表为不同的奇的单位分数之和.

Tenenbaum 和 Yokota 指出，m/n 可以表示成 r 个分母 $\leqslant 4n(\ln n)^2\log_2 n$ 的单位分数之和，其中 $r\leqslant(1+\varepsilon)\ln n/\log_2 n$，但 $1+\varepsilon$ 不能被 $1-\varepsilon$ 代替.

Victor Meally 把 0 和 1 之间的有理数 $a/b(a\perp b)$ 按照 $a+b$ 的大小和 a 的大小排序：$\frac{1}{2},\frac{1}{3},\frac{1}{4},\frac{2}{3},\frac{1}{5},\frac{1}{6},\frac{2}{5},\frac{3}{4},\cdots$. 注意：$\frac{2}{3}$，$\frac{4}{5}$ 和 $\frac{8}{11}$ 分别是此序列中最早需要用 2 个、3 个和 4 个单位分数来表示的元素. 哪些分数分别是最早需要用 5 个、6 个和 7 个单位分数来表示的呢？Stephane Vandemergel 在 1993 年 4 月 28 日的一封信中说：$\frac{16}{17}$ 要 5 个单位分数，而 $\frac{77}{79}$ 则要 6 个.

Barbeau 把 1 表示成 101 个不同的正整数的倒数之和，其中没有一个整数能整除另外的整数. Erdös 和 Graham 证明了：如果 n 无平方因子，那么 m/n 总可以写成有限多个无平方因子整数的倒数之和，其中每一个整数都恰有 ω 个($\omega\geqslant 3$)不同的素因子. 在许多情形可以取 ω 为 2. 对 $m=n=1$，至少需要 38 个整数：Allan Johson 对 $\omega=2$ 和下面 48 个数

6	21	34	46	58	77	87	115	155	215	287	391
10	22	35	51	62	82	91	119	187	221	299	689
14	26	38	55	65	85	93	123	203	247	319	731
15	33	39	57	69	86	95	133	209	265	323	901

完成了这一工作. 是否这就是最小可能的集合? Richard Stong 也解决了这个问题,但他用到一个更大的集合.

Erdös 在一封写于 1972 年 1 月 14 日的信中令$\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}=\frac{a}{b}$,这里 $b=[2,3,\cdots,n]$,即为 $2,3,\cdots,n$ 的最小公倍数. 他注意到$\frac{1}{2}+\frac{1}{3}=\frac{5}{6}$和$\frac{1}{2}+\frac{1}{3}+\frac{1}{4}=\frac{13}{12}$都使得有 $a\pm 1\equiv 0 \bmod b$,他问:这是否会再次出现? 他猜想不会. 是否无穷多次有 $a\perp b$ 呢?

如果 $\sum_{i=1}^{t} 1/x_i=1$,这里 $x_1<x_2<x_3<\cdots$ 是不同的正整数,Erdös 和 Graham 问 $m(t)$ 的值等于什么?这里 $m(t)=\min\max x_i$,其中最小值取过所有集合$\{x_i\}$. 例如 $m(3)=6, m(4)=12$, $m(12)=120$($m(12)=120$ 是不正确的——译者注). 是否对某个常数 c 有 $m(t)<ct$?按照这个记号,对所有 i 能有 $x_{i+1}-x_i\leqslant 2$ 吗?Erdös 猜想这不可能,并悬赏 10 美元给解决此问题者.

Erdös 和 Graham 问下述结论是否为真:用 c 种颜色对整数的任一种着色都给出

$$\sum \frac{1}{x_i}=1,\quad x_1<x_2<\cdots(\text{有限和})$$

的一个单色解(monocromatic solution)吗? 即使对 $c=2$,此问题也未解决. 如果答案是肯定的,令 $f(c)$是使整数 $1\leqslant t\leqslant f(c)$的每个 c-着色(c-coloring)都包含一个单色解的最小整数. 试确定 $f(c)$的值或估计它的大小.

Erdös 还问道:如果

$$\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_k}=1,\quad x_1<x_2<\cdots<x_k,$$

且 k 固定,那么 $\max x_1$ 等于什么? 如果 k 变化,什么整数能等于最大的分母 x_k? 不是素数,也不是 n 个其他的整数;被排除在外的整数有正密度吗? 甚至可以有密度 1? 什么整数可以是 x_k 或

x_{k-1}? 什么整数可以是 x_k 或 x_{k-1} 或 x_{k-2}? $\liminf \frac{x_k}{x_1} > e$ 吗? 平凡地有 $\liminf \frac{x_k}{x_1} \geqslant e$. 可能事实上它是无限的. 如果对每个 k, $m(k)$ 都等于 $\max(x_k)$,则 Yokota 改进了 Erdös 和 Graham 的一个结果,他证明了:存在一个整数 k 的递增序列,使有 $m(k)/k \leqslant (\ln \ln k)^3$. 是否存在 k 的一个序列使 $m(k)/k$ 有界呢?

Erdös 进一步问:是否对

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} = 1$$

的每个解都有 $\max(x_{i+1} - x_i) \geqslant 3$? $\{2,3,6\}$ 表明 >3 不真,但这似乎是惟一的反例. 可能 $\max(x_{i+1} - x_i) \leqslant c$ 仅有有限多个解. 如果 x_i 是 r 段连续整数的并集,那么解数有限且仅与 r 有关. Cuitiss 证明了:序列 $\frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{43} + \cdots$ 将 $\max x_k$ 作为 r 的函数给出.

如果 $N(n)$ 是可以表为 $\leqslant n$ 的不同整数的倒数之和的那种整数之集合,则 Yokota 证明了:直到

$$\frac{\ln n}{2}\left(1 - \frac{2\ln \ln n}{\ln n}\right)$$

为止的每个自然数都在 $N(n)$ 中,从而 $\# N(n) \geqslant \left(\frac{1}{2} + o(1)\right)\ln n$. Erdös 要求对不在 $N(n)$ 中的最小整数以及在 $N(n)$ 中的最大整数的大小给出一个估计. 有多少个整数 $< \sum_{i=1}^{n} 1/i$ 不能这样表示呢?在能这样表示的数中,它们的分布又如何?它们会成串地出现吗?

给定一个有正密度的序列 $x_1, x_2, \cdots$,是否总有有限子集满足 $\sum 1/x_{i_k} = 1$?如果对所有 i 有 $x_i < ci$,问存在这样一个有限子集吗?Erdös 再次悬赏 10 美元给解决此问题者. 如果 $\liminf x_i/i < \infty$,他坚定地猜想答案是否定的,并提供 5 美元给解决此问题者.

用 $N(t)$ 表示 $1=\sum 1/x_i$ 的解 $\{x_1,x_2,\cdots,x_t\}$ 的个数，而用 $M(t)$ 表示不同的解 $x_1\leqslant x_2\leqslant\cdots\leqslant x_t$ 的个数. Singmaster 计算出

t	1	2	3	4	5	6
$M(t)$	1	1	3	14	147	3462
$N(t)$	1	1	10	215	12231	2025462,

Erdös 要求给出 $M(t)$ 和 $N(t)$ 的渐近公式.

Graham 证明了:如果 $n>77$,我们可以把 $n=x_1+x_2+\cdots+x_t$ 分划成 t 个不同的正整数之和，使 $\sum 1/x_i=1$. 更一般地,对任何正有理数 α,β,存在一个整数 $r(\alpha,\beta)$(我们将取其最小的值),使得任何大于 r 的整数都能被分划成大于 β 的不同的正整数,这些正整数的倒数之和等于 α. 关于 $r(\alpha,\beta)$ 知道的很少,除了 D. H. Lehmer 的一篇未发表的论文,在这篇论文中他证明了:77 不能用这种方式划分,因此有 $r(1,1)=77$.

Graham 猜想:对充分大的 n(大约 10^4 这么大?),我们可以类似地划分 $n=x_1^2+x_2^2+\cdots+x_t^2$,使有 $\sum 1/x_i=1$. 我们还可以要求一个分解 $n=p(x_1)+p(x_2)+\cdots+p(x_t)$,其中 $p(x)$ 是任何"合理的"多项式.例如,x^2+x 就是不合理的,因为它仅取偶数值.

为了回答 L.-S. Hahn 的一个问题"是否存在一个整数集合，每个数都有一个与之相邻的数，它们的倒数之和是一个整数?",Peter Montgomery 给出了例子 {1,2,7,8,13,14,39,40,76,77,285,286} 和 {2,3,4,5,6,7,9,10,17,18,34,35,84,85},它们每一个的倒数之和都是 2.

L.-S. Hahn 又问:如果正整数用任何方式被划分成有限多个集合,是否总有一个集合存在,使任何正有理数都可以用它的有限多个不同的元素的倒数之和来表示? 这里一定有可能选取与该有理数无关的集合. 如果没有这种可能性,则给定任何有理数,是否总可以选取有此性质的一个集合呢? 现在这个集合与该有理数有关.

Nagell 证明了:一个算术级数的倒数之和恒不是整数，也见

Erdös 和 Niven 的论文.

参考文献

P. J. van Albada & J. H. van Lint, Reciprocal bases for the integers, *Amer. Math. Monthly*, **70**(1963) 170–174.

Michael Anshel & Dorian Goldfeld, Partitions, Egyptian fractions, and free products of finite abelian groups, *Proc. Amer. Math. Soc.*, **111**(1991) 889–899; *MR* **91h**:11104.

E. J. Barbeau, Remarks on an arithmetic derivative, *Canad. Math. Bull.*, **4**(1961) 117–122.

E. J. Barbeau, Computer challenge corner: Problem 477: A brute force program, *J. Recreational Math.*, **9**(1976/77) 30.

E. J. Barbeau, Expressing one as a sum of odd reciprocals: comments and a bibliography, *Crux Mathematicorum* (=*Eureka* (Ottawa)), **3**(1977) 178–181; and see *Math. Mag.*, **49**(1976) 34.

Laurent Beeckmans, The splitting algorithm for Egyptian fractions, *J. Number Theory*, **43**(1993) 173–185.

Leon Bernstein, Zur Lösung der diophantischen Gleichung $m/n = 1/x+1/y+1/z$ insbesondere im Falle $m = 4$, *J. reine angew. Math.*, **211**(1962) 1–10; *MR* **26** #77.

M. N. Bleicher, A new algorithm for the expansion of Egyptian fractions, *J. Number Theory*, **4**(1972) 342–382; *MR* **48** #2052.

M. N. Bleicher and P. Erdős, The number of distinct subsums of $\sum_1^N 1/i$, *Math. Comput.*, **29**(1975) 29–42 (and see *Notices Amer. Math. Soc.*, **20**(1973) A-516).

M. N. Bleicher and P. Erdős, Denominators of Egyptian fractions, *J. Number Theory*, **8**(1976) 157–168; *MR* **53** #7925; II, *Illinois J. Math.*, **20**(1976) 598–613; *MR* **54** #7359.

Robert Breusch, A special case of Egyptian fractions, Solution to Advanced Problem 4512, *Amer. Math. Monthly*, **61**(1954) 200–201.

J. L. Brown, Note on complete sequences of integers, *Amer. Math. Monthly*, **68**(1961) 557–560.

Paul J. Campbell, Bibliography of algorithms for Egyptian fractions (preprint), Beloit Coll., Beloit WI 53511, U.S.A.

Robert Cohen, Egyptian fraction expansions, *Math. Mag.*, **46** (1973) 76–80; *MR* **47** #3300.

D. R. Curtiss, On Kellogg's Diophantine problem, *Amer. Math. Monthly*, **29**(1922) 380–387.

Editor's Note, Odd reciprocals, *Math. Mag.*, **49**(1976) 155–156.

P. Erdős, Egy Kürschák-féle elemi számelméleti tétel áltadanositása, *Mat. es Fys. Lapok* **39**(1932).

P. Erdős, On arithmetical properties of Lambert series, *J. Indian Math. Soc.*, **12**(1948) 63–66.

P. Erdős, On a diophantine equation (Hungarian. Russian and English summaries), *Mat. Lapok*, 1(1950) 192–210; *MR* **13**, 208.

P. Erdős, On the irrationality of certain series, *Nederl. Akad. Wetensch. (Indag. Math.)* **60**(1957) 212–219.

P. Erdős, Sur certaines séries à valeur irrationelle, *Enseignement Math.*, **4**(1958) 93–100.

P. Erdős, *Quelques problèmes de la Théorie des Nombres*, Monographies de l'Enseignement Math. No. 6, Geneva, 1963, problems 72–74.

P. Erdős, Comment on problem E2427, *Amer. Math. Monthly*, **81**(1974) 780–782.

P. Erdős, Some problems and results on the irrationality of the sum of infinite series, *J. Math. Sci.*, **10**(1975) 1–7.

P. Erdős & I. Joó, On the expansion $1 = \sum q^{-n_i}$, *Period. Math. Hungar.*, **23**(1991) 27–30; *MR* **92i**:11030.

P. Erdős & Ivan Niven, Some properties of partial sums of the harmonic series, *Bull. Amer. Math. Soc.*, **52**(1946) 248–251; *MR* **7**, 413.

Paul Erdős & Sherman Stein, Sums of distinct unit fractions, *Proc. Amer. Math. Soc.*, **14**(1963) 126–131.

P. Erdős & E. G. Straus, On the irrationality of certain Ahmes series, *J. Indian Math. Soc.*, **27**(1968) 129–133.

P. Erdős & E. G. Straus, Some number theoretic results, *Pacific J. Math.*, **36**(1971) 635–646.

P. Erdős & E. G. Straus, Solution of problem E2232, *Amer. Math. Monthly*, **78**(1971) 302–303.

P. Erdős & E. G. Straus, On the irrationality of certain series, *Pacific J. Math.*, **55**(1974) 85–92; *MR* **51** #3069.

P. Erdős & E. G. Straus, Solution to problem 387, *Nieuw Arch. Wisk.*, **23**(1975) 183.

Nicola Franceschine, Egyptian Fractions, MA Dissertation, Sonoma State Coll. CA, 1978.

Charles N. Friedman, Sums of divisors and Egyptian fractions, *J. Number Theory*, **44**(1993) 328–339.

S. W. Golomb, An algebraic algorithm for the representation problem of the Ahmes papyrus, *Amer. Math. Monthly*, **69**(1962) 785–786.

S. W. Golomb, On the sums of the reciprocals of the Fermat numbers and related irrationalities, *Canad. J. Math.*, **15**(1963) 475–478.

R. L. Graham, A theorem on partitions, *J. Austral. Math. Soc.*, **3**(1963) 435–441; *MR* **29** #64.

R. L. Graham, On finite sums of unit fractions, *Proc. London Math. Soc.* (3), **14**(1964) 193–207; *MR* **28** #3968.

R. L. Graham, On finite sums of reciprocals of distinct nth powers, *Pacific J. Math.*, **14**(1964) 85–92; *MR* **28** #3004.

H. S. Hahn, Old wine in new bottles: Solution to E2327, *Amer. Math. Monthly*, **79**(1972) 1138 (and see Editor's comment).

Chao Ko, Chi Sun & S. J. Chang, On equations $4/n = 1/x + 1/y + 1/z$, *Acta Sci. Natur. Szechuanensis*, **2**(1964) 21–35.

Li De Lang, On the equation $4/n = 1/x+1/y+1/z$, *J. Number Theory*, **13**(1981) 485–494; *MR* **83e**:10026.

Liang-Shin Hahn, Problem E2689, *Amer. Math. Monthly*, **85**(1978) 47; Solution, Peter Montgomery & Dean Hickerson, **86**(1979) 224.

Liang-Shin Hahn, Problems and solutions (Japanese), *Sûgaku*, **31**(1979) 376.

Liang-Shin Hahn, Egyptian fractions (Chinese), *Mathmedia*, **15**(1980) 8–12.

Gerd Hofmeister & Peter Stoll, Note on Egyptian fractions, *J. reine angew. Math.*, **362**(1985) 141–145; *MR* **87a**:11025.

Allan Wm. Johnson, Letter to the Editor, *Crux Mathematicorum* (= *Eureka* (Ottawa)), **4**(1978) 190.

O. D. Kellogg, On a diophantine problem, *Amer. Math. Monthly*, **28**(1921) 300–303.

F. Mittelbach, Anzahl- und Dichteuntersuchungen bei Stammbruchdarstellungen von Brüchen, Diplomarbeit, Fachbereich Mathematik, Joh. Gutenberg-Univ., Mainz, 1988.

T. Nagell, *Skr. Norske Vid. Akad. Kristiania I*, 1923, no. 13 (1924) 10–15.

D. J. Newman, Problem 76-5: an arithmetic conjecture, *SIAM Rev.*, **18**(1976) 118.

R. Obláth, Sur l'équation diophantienne $4/n = 1/x_1 + 1/x_2 + 1/x_3$, *Mathesis*, **59**(1950) 308–316; *MR* **12**, 481.

J. C. Owings, Another proof of the Egyptian fraction theorem, *Amer. Math. Monthly*, **75**(1968) 777–778.

G. Palamà, Su di una congettura di Sierpiński relativa alla possibilità in numeri naturali della $5/n = 1/x_1 + 1/x_2 + 1/x_3$, *Boll. Un. Mat. Ital.*(3) **13**(1958) 65–72; *MR* **20** #3821.

G. Palamà, Su di una congettura di Schinzel, *Boll. Un. Mat. Ital.*(3) **14**(1959) 82–94; *MR* **22** #7989.

L. A. Rosati, Sull'equazione diofantea $4/n = 1/x_1 + 1/x_2 + 1/x_3$, *Boll. Un. Mat. Ital.*(3), **9**(1954) 59–63; *MR* **15**, 684.

J. W. Sander, On $4/n = 1/x+1/y+1/z$ and Rosser's sieve, *Acta Arith.*, **59**(1991) 183–204; *MR* **92j**:11031.

Andrzej Schinzel, Sur quelques propriétés des nombres $3/n$ et $4/n$, où n est un nombre impair, *Mathesis*, **65**(1956) 219–222; *MR* **18**, 284.

W. Schwarz, *Einführung in Siebmethoden der analytischen Zahlentheorie*, Bibl. Inst., Mannheim-Wien-Zurich, 1974; *MR* **53** #13147.

Jiří Sedláček, Über die Stammbrüche, *Časopis Pěst. Mat.*, **84**(1959) 188–197; *MR* **23** #A829.

W. Sierpiński, Sur les décompositions de nombres rationale en fractions primaires, *Mathesis*, **65**(1956) 16–32; *MR* **17**, 1185.

W. Sierpiński, *On the Decomposition of Rational Numbers into Unit Fractions* (Polish), Pánstwowe Wydawnictwo Naukowe, Warsaw, 1957.

W. Sierpiński, Sur une algorithme pour developper les nombres réels en séries rapidement convergentes, *Bull. Int. Acad. Sci. Cracovie Ser. A Sci. Math.*, **8**(1911) 113–117.

David Singmaster, The number of representations of one as a sum of unit fractions (mimeographed note), 1972.
B. M. Stewart, Sums of distinct divisors, *Amer. J. Math.*, **76**(1954) 779–785; *MR* **16**, 336.
B. M. Stewart & W. A. Webb, Sums of fractions with bounded numerators, *Canad. J. Math.*, **18**(1966) 999–1003; *MR* **33** #7297.
R. J. Stroeker & R. Tijdeman, Diophantine equations, *Computational Methods in Number Theory, Part II*, Math. Centrum Tracts **155**, Amsterdam, 1982; *MR* **84i**:10014.
J. J. Sylvester, On a point in the theory of vulgar fractions, *Amer. J. Math.*, **3**(1880) 332–335, 387–388.
Gérald Tenenbaum & Hisashi Yokota, Length and denominators of Egyptian fractions III, *J. Number Theory*, **35**(1990) 150–156; *MR* **91g**:11028.
R. C. Vaughan, On a problem of Erdős, Straus and Schinzel, *Mathematika*, **17**(1970) 193–198.
H. S. Wilf, Reciprocal bases for the integers, Res. Problem 6, *Bull. Amer. Math. Soc.*, **67**(1961) 456.
Koichi Yamamoto, On the diophantine equation $4/n = 1/x + 1/y + 1/z$, *Mem. Fac. Sci. Kyushū Univ. Ser. A*, **19**(1965) 37–47.
Koichi Yamamoto, On a conjecture of Erdős, *Mem. Fac. Sci. Kyushū Univ. Ser. A*, **18**(1964) 166–167; *MR* **30** #1968.
Hisashi Yokota, On number of integers representable as sums of unit fractions, *Canad. Math. Bull.*, **33**(1990) 235–241; *MR* **909**:11029.
Hisashi Yokota, On a problem of Erdős and Graham, *J. Number Theory*, **39**(1991) 327–338; *MR* **90d**:11104.

D12. Markoff 数

一个产生了巨大兴趣的不定方程是

$$x^2 + y^2 + z^2 = 3xyz.$$

它显然有 Cassels 所说的奇异解(1,1,1)和(1,1,2)(由通常关于奇解的定义,该簇只有惟一的奇解(0,0,0)). 由于方程关于每个变量都是二次的,它所有的解都可以从上述的解生成,故而从一个整数解可以导出第二个整数解,而且可以证明:除了奇解外,所有解的 x,y,z 都有不同的值,因此每个这样的解都是恰好 3 个其他的解的邻伴(neighbor), 见图 10. 数 1,2,5,13,29,34,89,169,194,233,433,610,985,…称为 **Markoff 数**. 为避免平凡的结果,我们假设 $0<x\leqslant y\leqslant z$(从而如果 $y\geqslant 2$,该不等式是严格的). 一个出

色的问题是:是否每个 Markoff 数 z 定义一个惟一的整数解(x, y, z)? 不时有人声明他们证明了在此意义下 Markoff 数是惟一的,但是到目前为止的证明都是错的.

如果 $M(N)$是满足 $x\leqslant y\leqslant z\leqslant N$ 的三数组的个数,则 Zagier 证明了有 $M(N)=C(\ln N)^2+O((\ln N)^{1+\epsilon})$,其中 $C\approx 0.180717105$,计算引导他猜想:第 n 个 Markoff 数 m_n 的大小是 $\left(\frac{1}{3}+O(n^{-1/4+\epsilon})\right)A^{\sqrt{n}}$, 这里 $A+e^{1/\sqrt{C}}\approx 10.5101504$. 关于相异性,他没有得到什么结果,但是他能证明该问题等价于某种不定方程组的不可解性.

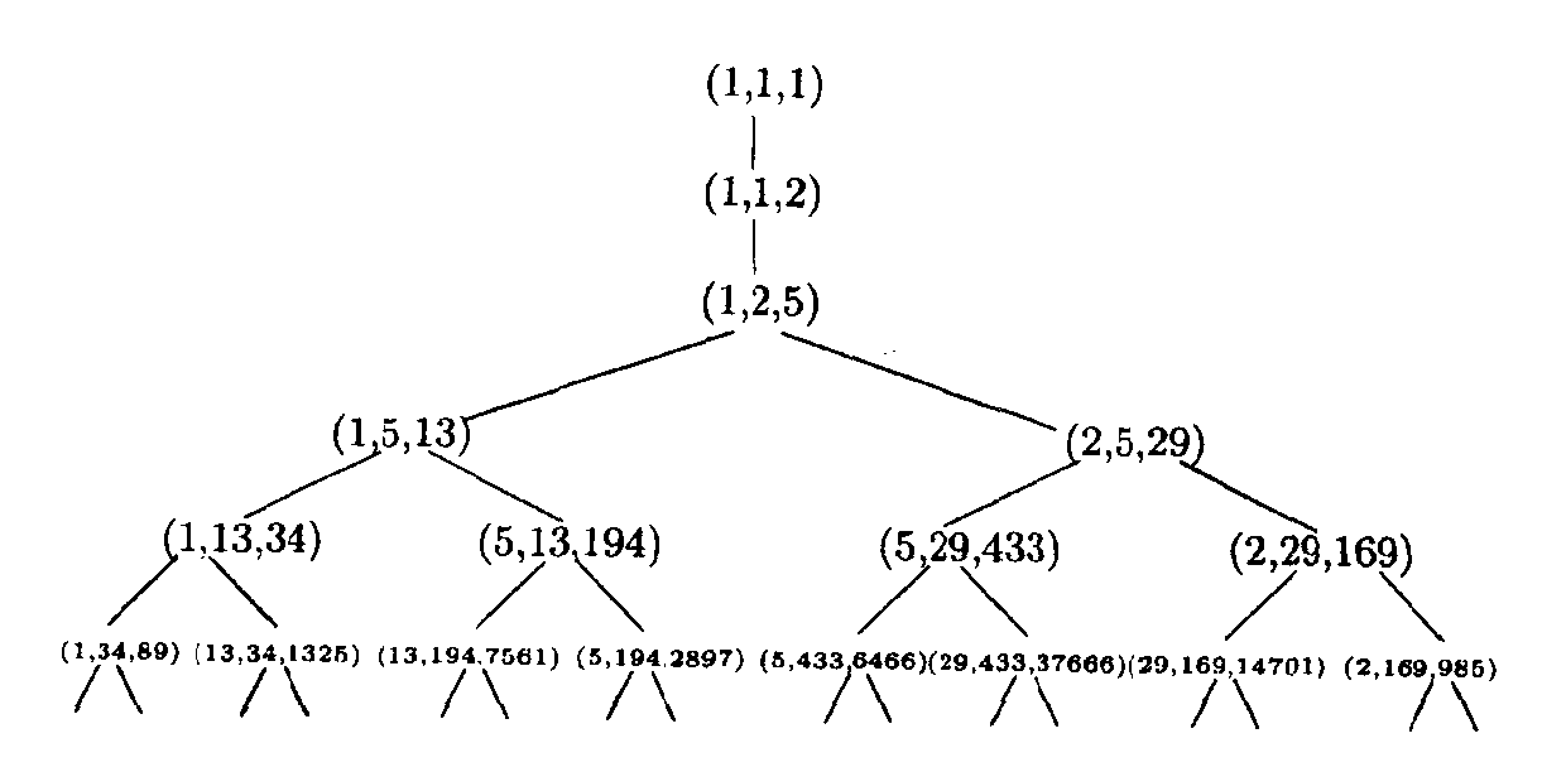


图 10　Markoff 解的树

Markoff 方程是更一般的 **Hurwitz 方程**(Hurwitz equation)

$$x_1^2+x_2^2+\cdots+x_n^2=ax_1x_2\cdots x_n$$

的特例,如果 $a>n$,它没有整数解;如果 $a=n$,所有整数解可以由$(1,1,\cdots,1)$生成. 对任何 a, $1\leqslant a\leqslant n$,都有一组有限的解集,由它可以生成所有其他的解. Baragar 证明了:对任何 g,存在无穷多对(a,n),使得方程至少要求 g 个生成元. 令 $M(n,N)$是$a=n$ 时 Hurwitz 方程的解数,且每一个$|x_i|\leqslant N$,则 Baragar 也证明了:对所有 $\epsilon>0$, $M(n,N)$像 $C(\ln N)^{\alpha(n)+\epsilon}$一样增长,且 $M(n,N)$

$=\Omega(\ln N)^{\alpha(n)-\varepsilon}$)，这里(Zagier) $\alpha(3)=2$，但是 $\alpha(4)$在 2.33 和 2.64之间(稍后改进为 $2.43<\alpha(4)<2.47$)．他还证明了

$$\frac{2\ln n}{\ln 4}\leqslant\alpha(n)\leqslant\frac{3\ln n}{\ln 4}.$$

参考文献

Arthur Baragar, The Hurwitz equations, Proc. Conf. Markoff Spectrum & Anal. Number Theory, Provo UT, 1991; Lect. Notes Pure Appl. Math., **147** 9–16, Dekker, New York, 1993.

J. W. S. Cassels, An Introduction to Diophantine Approximation, Cambridge, 1957, 27–44.

H. Cohn, Approach to Markoff's minimal forms through modular functions, *Ann. Math. Princeton*(2) **61**(1955) 1–12; *MR* **16**, 801e.

T. W. Cusick, The largest gaps in the lower Markoff spectrum, *Duke Math. J.*, **41**(1974) 453–463; *MR* **57** #5902.

T. W. Cusick, On Perrine's generalized Markoff equations, *Aequationes Math.*, **46**(1993) 203–211.

L. E. Dickson, *Studies in the Theory of Numbers*, Chicago Univ. Press, 1930, Chap. VII.

G. Frobenius, Über die Markoffschen Zahlen, *S.-B. Preuss. Akad. Wiss. Berlin* (1913) 458–487.

Norman P. Herzberg, On a problem of Hurwitz, *Pacific J. Math.*, **50**(1974) 485–493; *MR* **50** #233.

A. Hurwitz, Über eine Aufgabe der unbestimmten Analysis, *Arch. Math. Phys.*, **3**(1907) 185–196; *Math. Werke*, ii, 410–421.

A. Markoff, Sur les formes quadratiques binaires indéfinies, *Math. Ann.*, **15**(1879) 381–409.

Serge Perrine, Sur une généralisation de la théorie de Markoff, *J. Number Theory*, **37**(1991) 211–230; *MR* **92c**:11067.

R. Remak, Über indefinite binäre quadratische Minimalformen, *Math. Ann.*, **92**(1924) 155–182.

R. Remak, Über die geometrische Darstellung der indefiniten binären quadratischen Minimalformen, *Jber. Deutsch Math.-Verein*, **33**(1925) 228–245.

Gerhard Rosenberger, The uniqueness of the Markoff numbers, *Math. Comput.*, **30**(1976) 361–365; but see *MR* **53** #280.

Joseph H. Silverman, The Markoff equation $X^2+Y^2+Z^2=aXYZ$ over quadratic imaginary fields, *J. Number Theory*, **35**(1990) 72–104; *MR* **91i**:11028.

L. Ja. Vulah, The diophantine equation $p^2+2q^2+3r^2=6pqr$ and the Markoff spectrum (Russian), *Trudy Moskov. Inst. Radiotehn. Èlektron. i Avtomat. Vyp. 67 Mat.*(1973) 105–112, 152; *MR* **58** #21957.

Don B. Zagier, On the number of Markoff numbers below a given bound *Math. Comput.*, **39**(1982) 709–723; *MR* **83k**:10062.

D13. 方程 $x^x y^y = z^z$

Erdös 要求方程 $x^x y^y = z^z$ 的除了平凡解 $y=1, x=z$ 以外的解. 柯召(Chao Ko)找到了无穷多个解,其中头 3 个是

x	y	z
12^6	6^8	$2^{11}3^7$
224^{14}	112^{16}	$2^{68}7^{15}$
61440^{30}	30720^{32}	$2^{357}15^{31}$.

他找到了全部的解吗?

Claude Anderson 猜想,方程 $w^w x^x y^y = z^z$ 没有满足 $1 < w < x < y < z$ 的解,但是,柯召和孙琦(Sun Qi)早先就对这一猜想向任意多个变量作的一个推广找到了无穷多个反例:

$$x_1 = k^{k^n(k^{n+1}-2n-k)+2n}(k^n - 1)^{2(k^n-1)}$$

$$x_2 = k^{k^n(k^{n+1}-2n-k)}(k^n - 1)^{2(k^n-1)+2}$$

$$x_3 = \cdots = x_k = k^{k^n(k^{n+1}-2n-k)+n}(k^n - 1)^{2(k^n-1)+1}$$

$$z = k^{k^n(k^{n+1}-2n-k)+n+1},$$

这里,对 $k \geqslant 3$ 有 $n > 0$,而对 $k=2$ 则有 $n > 1$. 例如,$w = 3^{12}2^6$, $x = 3^{13}2^5$, $y = 3^{14}2^4$, $z = 3^{14}2^5$. Ajai Choudhry 对 $k=3$ 也找到了一个参数解.

参 考 文 献

Chao Ko, Note on the diophantine equation $x^x y^y = z^z$, *J. Chinese Math. Soc.*, **2**(1940) 205–207; *MR* **2**, 346.

Chao Ko & Sun Qi, On the equation $\prod_{i=1}^{k} x_i^{x_i}$, *J. Sichuan Univ.*, **2**(1964) 5–9.

W. H. Mills, An unsolved diophantine equation, *Report Inst. Theory of Numbers*, Boulder CO, 1959, 258–268.

D14. a_i+b_j 作成平方数

Leo Moser 要求整数 $a_1,a_2,b_j(1\leqslant j\leqslant n)$，使得 $2n$ 个数 a_i+b_j都是平方数. 取 a_2-a_1 是充分复合的数就可以达此目的. 例如，$a_1=0,a_2=2^{2n+1},b_j=(2^{2n-j}-2^{j-1})^2$.

John Leech 注意到，推广到整数 $a_1,a_2,a_3,b_j(1\leqslant j\leqslant n)$，问题对任何 n 也可解. 我们可取 a_1,a_2 是$(x\pm y)^2$，a_3 可以取任意的值 $x^2+\lambda xy+y^2$(它可以通过令 $x=u^2-v^2,y=2uv+\lambda v^2$ 而成为平方数). u 和 v 的任何值将会给这 3 个平方数的差以相等的比例. 求 u 和 v 的值使得比例因子是一个有理平方数的问题归结为求一条椭圆曲线上的有理点，对任何 n，b_j 的任意多个有理值可以同时通过调节而给出整数$a_1,a_2,a_3,b_j(1\leqslant j\leqslant n)$. 研究得很多的一种情形是 $\lambda=0$，它对应于若干组有相等面积的有理直角三角形. 我们还可以特别地固定 $a_1=b_1=0$. 只要 a_2,a_3 是平方数 p^2,q^2，使得 q/p 可以表为两个不同的比值$(u^2-v^2)/2uv$ 的乘积，那么，求有理平方数 $b_j=r_j^2$ 使 $p^2+r_j^2$ 和 $q^2+r_j^2$ 两者都是平方数的问题再次是一个椭圆曲线的问题，我们又可以重新调节以便对任何 n 求得整数 $p,q,r_j(1\leqslant j\leqslant n)$，使得 $p^2+r_j^2$ 和 $q^2+r_j^2$ 都是整数的平方(参见 D20). 例如，13/6 有表示$(u_1,v_1,u_2,v_2)=(9,4,5,1)$和$(8,5,9,1)$，它们生成：

$$\begin{array}{ccccc} 0^2 & 351^2 & 650^2 & 1728^2 & 3200^2 \\ 720^2 & 801^2 & 970^2 & 1872^2 & 3280^2 \\ 1560^2 & 1599^2 & 1690^2 & 2328^2 & 3560^2. \end{array}$$

更为一般地，我们寻求整数 $a_i(1\leqslant i\leqslant m),b_j(1\leqslant j\leqslant n)$. Jean Lagrange 造出了二次型$(a,b,c)=au^2+buv+cv^2$ 的平方的矩阵：

$$\begin{pmatrix} (54,150,111)^2 & (56,150,79)^2 & (72,234,177)^2 & (72,186,57)^2 \\ (6,78,96)^2 & (16,48,56)^2 & (48,192,168)^2 & (48,120,12)^2 \\ (54,318,384)^2 & (56,312,376)^2 & (72,360,408)^2 & (72,312,372)^2 \\ (6,-50,-96)^2 & (16,0,-56)^2 & (48,176,168)^2 & (48,104,-12)^2 \end{pmatrix}$$

它对 $m=n=4$ 产生无穷多个解. 例如,$u=2,v=1$ 给出:

$$\begin{pmatrix} 627^2 & 603^2 & 933^2 & 717^2 \\ 276^2 & 216^2 & 744^2 & 444^2 \\ 1236^2 & 1224^2 & 1416^2 & 1284^2 \\ 172^2 & 8^2 & 712^2 & 388^2 \end{pmatrix}$$

Lagrange 在一封 1983 年 3 月 13 日的信中给出矩阵:

$$\begin{pmatrix} 59^2 & 112^2 & 144^2 & 207^2 & 592^2 & 1351^2 & 4077^2 \\ 229^2 & 248^2 & 264^2 & 303^2 & 632^2 & 1369^2 & 4083^2 \\ 499^2 & 508^2 & 516^2 & 537^2 & 772^2 & 1439^2 & 4107^2 \end{pmatrix}$$

和

$$\begin{pmatrix} 18^2 & 234^2 & 346^2 & 514^2 \\ 282^2 & 366^2 & 446^2 & 586^2 \\ 477^2 & 531^2 & 589^2 & 701^2 \\ 1122^2 & 1146^2 & 1174^2 & 1234^2 \end{pmatrix}$$

在这些例子中,a_i,b_j 不是平方数. 如果 a_i,b_j 本身是平方数,那么它们就提供了与问题 D20 有关的构形(见 D20),在这方面 Lagrange 和 Leech 做出了相当的进展. 他们的平方数的三数组 $a_i^2(i=1,2,3)$ 和四数组 $b_j^2(j=1,2,3,4)$ 及所有 $a_i^2+b_j^2$ 皆为平方数合在一起引导到本问题中的 4×5 阵列

$$\begin{pmatrix} 0^2 & 7422030^2 & 8947575^2 & 22276800^2 & 44142336^2 \\ 9282000^2 & 11184530^2 & 12892425^2 & 24132200^2 & 45107664^2 \\ 26822600^2 & 27830530^2 & 28275625^2 & 34867000^2 & 51652664^2 \\ 60386040^2 & 60840450^2 & 61045335^2 & 64364040^2 & 74799864^2 \end{pmatrix}$$

D15. 每对数的和均为平方数的数组

Erdös 和 Leo Moser(见较早的文献)也问到类似的问题:对每个 n,存在 n 个不同的数使任一对数的和都是平方数吗? 对 $n=3$ 我们可以取

$$a_1 = \frac{1}{2}(q^2 + r^2 - p^2),$$

$$a_2 = \frac{1}{2}(r^2 + p^2 - q^2),$$

$$a_3 = \frac{1}{2}(p^2 + q^2 - r^2).$$

而对 $n=4$ 我们可以取 s 为任何可以用三种不同方式表为两个平方数之和的数:

$$s = u^2 + p^2 = v^2 + q^2 = w^2 + r^2,$$

而

$$a_4 = s - \frac{1}{2}(p^2 + q^2 - r^2),$$

由此可以增加问题中数的个数.

对 $n=5$, Jean Lagrange 给出一个相当一般的参数解及其简化,这一简化似乎给出全部解中的大多数. 他列出了由 J. -L. Nicolas 计算出的头 80 个解. 最小的解是

$$-4878 \quad 4978 \quad 6903 \quad 12978 \quad 31122,$$

而最小的正解(每个解中至多可以有一个数是负的)是

$$7442 \quad 28658 \quad 148583 \quad 177458 \quad 763442.$$

在一封 1972 年 5 月 19 日的信中,他对 $n=6$ 给出下面的解:

$$-15863902 \quad 17798783 \quad 21126338$$

$$49064546 \quad 82221218 \quad 447422978.$$

实际上此问题可追溯到 T. Baker,他找到 5 个整数,其两两相加的和都是平方数;也可追溯到 C. Gill,他找到 5 个数,每 3 个数的和都是平方数.

Lagrange 还找到若干个集合,每个集合由 n 个平方数组成,每组中任何 $n-1$ 个数的和都是平方数. 对 $n=3,5$ 和 8,最小的这样的数分别是(44,117,240),(28,64,259,392,680)和(79,112,204,632,896,916,1828,2092)中诸数的平方.

Martin LaBar 要求证明或推翻下述结论:3×3 魔方可以用 9 个不同的整数的平方构造出来. 这要求 9 个量 x^2, y^2, z^2, y^2+z^2

$-x^2, z^2+x^2-y^2, x^2+y^2-z^2, 2x^2-y^2, 2x^2-z^2, 3x^2-y^2-z^2$ 是不同的完全平方数. 这不太像是对的，尽管不难做到使 8 个魔和中的 4 个符合要求.

参考文献

T. Baker, *The Gentleman's Diary* or *Math. Repository*, London, 1839, 33–35, Question 1385.

C. Gill, *Application of the Angular Analysis to Indeterminate Problems of Degree 2*, New York, 1848, p. 60.

Martin LaBar, Problem 270, *Canad. Math. J.*, **15**(1984) 69.

Jean Lagrange, Cinq nombres dont les sommes deux à deux sont des carrés, *Séminaire Delange-Pisot-Poitou* (*Théorie des nombres*) 12ᵉ *année*, **20**(1970-71) 10pp.

Jean Lagrange, Six entiers dont les sommes deux à deux sont des carrés, *Acta Arith.*, **40**(1981) 91–96.

Jean Lagrange, Sets of n squares of which any $n-1$ have their sum square, *Math. Comput.*, **41**(1983) 675–681.

Jean-Louis Nicolas, 6 nombres dont les sommes deux à deux sont des carrés, *Bull. Soc. Math. France*, Mém. No 49–50 (1977) 141–143; *MR* **58** #482.

A. R. Thatcher, A prize problem, *Math. Gaz.*, **61**(1977) 64.

A. R. Thatcher, Five integers which sum in pairs to squares, *Math. Gaz.*, **62**(1978) 25.

D16. 有相同和及相同积的三数组

求尽可能多的正整数的不同的三数组，使每组 3 个数有相同的和又有相同的积这一问题已由 Schinzel 解决：你可以找到任意多组. 其间 Stephane Vandemergel 也找到了 13 组三数组，每组中 3 个数的和是 17116，积是 $2^{10}3^3 5^2 7^2 11 \cdot 13 \cdot 19$. 对每种重数的数组，求出数组中诸数的最小的和或者最小的积，或许是有意义的. 例如，对 4 重三数组，J. G. Mauldon 找出最小的共同的和是 118：(14,50,54)，(15,40,63)，(18,30,70)，(21,25,72)；而最小的共同的乘积是 25200：(6,56,75)，(7,40,90)，(9,28,100)，(12,20,105).

参考文献

Lorraine L. Foster & Gabriel Robins, Solution to Problem E2872, *Amer. Math. Monthly*, **89**(1982) 499–500.

J. G. Mauldon, Problem E2872, *Amer. Math. Monthly*, **88**(1981) 148.

D17. 相连整数段之积不是幂

Erdös 和 Selfridge 证明了:相连整数的乘积绝不会是一个幂,又对 $n \geqslant 2k \geqslant 8$,二项系数 $\binom{n}{k}$(见 B31)也绝不会是一个幂. 如果 $k=2$,则 $\binom{n}{k}$ 无穷多次是一个平方数.但是 Tijdeman 的方法(见 D9)有可能证明它绝不会是一个非平凡的更高次幂(对三次和四次幂,见 Mordell 的书),而对 $k=3$,除了 $n=50$ 以外(见 D3),它也绝不是一个幂.

Erdös 和 Graham 问:两个或多个不相交的相连整数段的乘积是否能是一个幂? Pomerance 注意到,如果 $a_1=2^{n-1}$, $a_2=2^n$, $a_3=2^{2n-1}-1$, $a_4=2^{2n}-1$,那么

$$\prod_{i=1}^{4}(a_i-1)a_i(a_i+1)$$

是一个平方数.但是 Erdös 和 Graham 认为,如果 $l \geqslant 4$,那么仅在有限多个情形 $\prod_{i=1}^{k}\prod_{j=1}^{l}(a_i+j)$ 是一个平方数.

K. R. S. Sastry 注意到:如果 $(n+1)(2n-1)=m^2$,那么相连整数段 $(n-1)n(n+1)$ 与 $(2n-2)(2n-1)2n$ 的乘积是一个平方数. 这等价于一个有无穷多解的 Pell 方程. 例如,$n=74$ 给出

$$(73 \cdot 74 \cdot 75)(146 \cdot 147 \cdot 148) = 73^2 \cdot 74^2 \cdot 210^2.$$

Erdös 又问:(多于一个)相连奇数的乘积是否永远不是一个(高于一次的)幂? 一个算术级数的 4 个相连的元素的乘积是否永远不是一个幂? Euler 证明了它不可能是平方数. Fermat 证明了

其成员单个来说都不能是平方数，但一个非平方数的因子必定整除两个不同的项，或者：(a)2 整除第一和第三项，或者整除第二和第四项；或者(b)3 整除第一和第四项；或者(a)与(b)两者都成立.(a)不可能单独对模 8 成立；(b) 不可能单独对模 3 成立，但是我们可以有 $6t^2, u^2, 2v^2, 3w^2$. 不过这蕴含 $w^2+t^2=v^2$ 和 $w^2+4t^2=u^2$，它们可以用递降法来反证——一个毕达哥拉斯比值不可能是另一个的两倍. 对更高次幂，Leech 注意到：在算术级数中不能有 3 个立方数.

Sastry 问：对什么样的 k，一个算术级数的 4 个相连项的乘积能是一个 k 边形数？这里第 r 个 k 边形数(k-gonal number)是

$$\frac{1}{2}r((k-2)r-(k-4)).$$

注意，对 $k=4$，结果恰如 Euler 所证明的，但是 Sastry 对除了 7，14 和 37 以外所有其他的 k 都求得了解. 对于提到的这几个数不可能有解吗？

参考文献

P. Erdős, On consecutive integers, *Nieuw Arch. Wisk.*, **3**(1955) 124–128.
P. Erdős & J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.*, **19**(1975) 292–301.

D18. 有完全长方体吗？两两的和均为平方数的 4 个平方数；差为平方数的 4 个平方数

有有理的盒子吗？我们对这个名声显赫的未解决的问题的处理几乎完全归功于 John Leech. 是否存在一个有整数边长 x_i、整数面对角线长 y_i 和整数体对角线长 z 的完全长方体(perfect cuboid)呢？联立不定方程

(A) $$x_{i+1}^2 + x_{i+2}^2 = y_i^2,$$

(B) $$\sum x_i^2 = z^2$$

($i=1,2,3$；在必要时，下标按模 3 化简)有解吗？

Martin Gardner 问：是否 x_i, y_i, z 中任何 6 个数都能是整数？这里有 3 个问题：仅仅体对角线长 z 是无理数；仅有一条边 x_3 的长是无理数；恰有一条面对角线长 y_1 是无理数.

问题 1　我们要求(A)中 3 个问题的解. 设这样的解有生成元(generator) a_i, b_i，其中

$$x_{i+1} : x_{i+2} : y_i = 2a_ib_i : a_i^2 - b_i^2 : a_i^2 + b_i^2.$$

那么我们希望得到

$$\text{(C)} \qquad \prod \frac{a_i^2 - b_i^2}{2a_ib_i} = 1$$

的整数解. 我们可以假设诸生成元对有相反的奇偶性，并用

$$\text{(D)} \qquad \frac{a_1^2 - b_1^2}{2a_1b_1} \cdot \frac{a_2^2 - b_2^2}{2a_2b_2} = \frac{\alpha^2 - \beta^2}{2\alpha\beta}$$

代替(C). 一个例子是

$$\text{(E)} \qquad \frac{6^2 - 5^2}{2 \cdot 6 \cdot 5} \cdot \frac{11^2 - 2^2}{2 \cdot 11 \cdot 2} = \frac{8^2 - 5^2}{2 \cdot 8 \cdot 5}.$$

Kraitchik 给出边长为奇数且小于一百万的 241 + 18 − 2 个长方体. Lal 和 Blundon 列出了由(D)能得到的适合 $a_1, b_1; \alpha, \beta \leqslant 70$ 的所有的解，包括一对奇特的解(1008，1100，1155)和(1008，1100，12075)（译者注：$1008^2 + 1100^2 = 1492^2$，$1100^2 + 1155^2 = 1595^2$，$1155^2 + 1008^2 = 1533^2$，$1100^2 + 12075^2 = 12125^2$，$12075^2 + 1008^2 = 12117^2$，）. Leech 存储了一张表，这张表给出了从(D)中得到的有两对生成元且适合 $a_1, b_1; a_2, b_2; \alpha, \beta \leqslant 376$ 的所有解.

将(C)中下标的循环次序反过来就产生出**导出长方体**(derived cuboid)：例子(E)给出最小的解(240，44，117)(Euler 知道这一结果)以及导出长方体(429，2340，880). 注意有 $240 \cdot 429 = 44 \cdot 2340 = 117 \cdot 880$.

有若干个参数解是已知的：最简单的(也是 Euler 知道的)一个参数解是

$$\text{(F)} \qquad \alpha = 2(p^2 - q^2), \quad a_1 = 4pq, \quad b_1 = \beta = p^2 + q^2.$$

对固定的 a_1, b_1，(D)等价于平面三次曲线

$$\frac{a_1^2-b_1^2}{2a_1b_1}=\frac{u^2-1}{2u}\cdot\frac{2v}{v^2-1},$$

它的有理点是有限生成的，Mordell 告诉我们：由一个解即可导出无穷多个解．但并非所有的有理数 a_1/b_1 都出现在解中：$a_1/b_1=2$ 是不可能的，因而不存在一个有理长方体，它有一对边的比值是 3:4.

问题 2　仅有一条边长是无理数．我们希望有 $x_1^2+x_2^2=y_3^2$，而 $t+x_1^2, t+x_2^2, t+y_3^2$ 全都是平方数．这是由"Mahatma"(参见后面的参考文献——译者注)提出来的，而读者给出了 $x_1=124$，$x_2=957, t=13852800$. Bromhead 将此扩大到一个参数解．有无穷多个解由

(G)　$(x_1,x_2,y_3)=2\xi\eta\zeta(\xi,\eta,\zeta),\ t=\zeta^8-6\xi^2\eta^2\xi^4+\xi^4\eta^4$

给出，这里(ξ,η,ζ)是一个毕达哥拉斯三数组，其中最小的是 $\xi=5, \eta=12$; $x_1=7800, x_2=18720$; $t=211773121$. 较早时候 Flood 给出过一个解.

这些还没有完．我们来求

(H)　$$x_1^2+x_2^2=y_3^2,\quad z=x_1^2+y_1^2=x_2^2+y_2^2$$

的异于 $z=y_3(t=0)$的解．Leech 找到 100 个满足 $z<10^5$ 的本原解，其中 46 个有 $t>0$. (H)的生成元满足

(I)　$$\frac{\alpha_1^2+\beta_1^2}{2\alpha_1\beta_1}\cdot\frac{2\alpha_2\beta_2}{\alpha_2^2+\beta_2^2}=\frac{a^2-b^2}{2ab},$$

因此对固定的 x_2/x_1，它的解对应于三次曲线

(J)　$$x_1v(u^2+1)=x_2u(v^2+1)$$

上的有理点．平凡解 $t=0$ 对应于若干个寻常点(ordinary point)，对每个比值 x_2/x_1，这些寻常点生成无穷多个解．其解作成长为 4 的圈：

(K)　$$\zeta^2=\xi_1^2+\eta_1^2=\xi_2^2+\eta_2^2=\xi_3^2+\eta_3^2=\xi_4^2+\eta_4^2,$$
$$\xi_1\xi_3=\xi_2\xi_4,$$

$$\xi_1^2+\xi_2^2, \xi_2^2+\xi_3^2, \xi_3^2+\xi_4^2, \xi_4^2+\xi_1^2 \quad \text{都是平方数,}$$

这些圈对应于两对比值 x_2/x_1，它们对应于(J)上与点 $t=0$ 共线的两个点. 反过来说，这样的一对点对应于 4 个解组成的一个圈.

问题 3 恰有一条面对角线长为无理数. 这里有两个密切相关的问题：求 3 个其和与差均为平方数的整数；求 3 个其差为平方数的平方数. 该问题表为长方体的形式即是求满足

(L) $\quad x_2^2+y_2^2=z^2, \quad x_1^2+x_3^2=y_2^2, \quad x_1^2+x_2^2=y_3^2$

的整数，它的生成元满足

(M) $$\frac{\alpha_1^2-\beta_1^2}{2\alpha_1\beta_1}\cdot\frac{\alpha_3^2-\beta_3^2}{2\alpha_3\beta_3}=\frac{\alpha_2^2+\beta_2^2}{2\alpha_2\beta_2}.$$

记 $u_i=(\alpha_i^2-\beta_i^2)^2/4\alpha_i^2\beta_i^2$，则(M)变成 $u_1u_3=1+u_2$，这是一个在**圈**(cycle)和**装饰图案**(frieze pattern)方面被许多人研究过的方程. 解也出现在长为 5 的圈中！Leech 列出了 35 个适合 $\alpha_1,\beta_1,\alpha_2,\beta_2\leqslant 50$ 的解，并在未发表的数学表中储存了一张表，这张表上有适合两对数 $\alpha_i,\beta_i\leqslant 376$ 的所有的圈. 这和 Napier 的法则(有关 Napier 法则或 Napier 公式，请参看科学出版社出版的译著《数学百科全书》第四卷 p. 948～949——译者注)以及有理球面三角形的构造有密切的联系.

当 $(p^2-q^2)/2pq$ 和 $(r^2-s^2)/2rs$ 的分子和分母的乘积皆为平方数时，(L)的解由 $x_2^2=z^2-y_2^2=(p^2-q^2)(r^2-s^2)$，$x_3^2=z^2-y_3^2=4pqrs$ 给出. Euler 令 p,q,r,s 为平方数，他找到了四次幂的差，例如 $3^4-2^4, 9^4-7^4, 11^4-2^4$，它们两两的乘积都是平方数. 头两个数给出了这种类型的第二个最小的解(117,520,756)，它的圈包括最小的解(104,153,672)，这个解也是 Euler 所知道的.

我们还可以用两种不同的方式把 $z^2=x_2^2+y_2^2=x_3^2+y_3^2$ 表示成两个平方数的和：

$$x_3/x_1=(\alpha_2^2-\beta_2^2)/2\alpha_2\beta_2, \quad x_2/x_1=(\alpha_3^2-\beta_3^2)/2\alpha_3\beta_3,$$

这给出 $z^2=4(\alpha_2^2\alpha_3^2+\beta_2^2\beta_3^2)(\alpha_2^2\beta_3^2+\alpha_3^2\beta_2^2)$. Euler 把每一个因子作成平方数，从而找到了两个有相等面积 $\frac{1}{2}\alpha_2\alpha_3\beta_2\beta_3$ 的有理直角三

角形. Diophantus 用 $\beta_2/\alpha_2=(s+t)/2r$, $\beta_3/\alpha_3=s/t$ 解决了这一问题,其中 $r^2=s^2+st+t^2$, $s=l^2-m^2$, $t=m^2-n^2$. 令 $(l,m,n)=(1,2,-3)$,我们就得到一个圈,这个圈包含这些长方体中第三、第四以及第五个最小的长方体. Leech 找到 89 个满足 $z<10^5$ 的解.

对固定的 α_1/β_1,在曲线

$$(\alpha_1^2-\beta_1^2)u(v^2-1)=2\alpha_1\beta_1 v(u^2+1)$$

上有(M)的与一个寻常点对应的非平凡的解,它生成无穷多个解. 在该点的切线生成一个特别有意思的圈.

(M)很像(D),但是不像(I),它并非对所有的比值 α/β 都有非平凡的解. 例如,对 $\alpha/\beta=2$ 或 3 就没有,从而再次没有边长的比为 3:4 的长方体. 这里没有"导出"长方体.

对于积和商都是平方数的比值 $(p^2-q^2)/2pq$,两个另外的参数形式是

$$p=2m^2\pm n^2,\quad r=m^2\pm 2n^2,\quad q=s=m^2\mp n^2.$$

两两的和均为平方数的 4 个平方数. (C)的一个解给出 3 个这样的平方数. 它可以被描述成一个图的三阶**顶点**(vertex),把它连接到**结点**(node)的三条边代表有理三角形的生成元对. 如果这样一对生成元在一个解中出现了,它就会在无穷多个解中出现,故一个结点的阶是无限的. 我们要寻找一个与四面体 K_4 同胚的子图,其顶点给出(C)的四个解,且它的边包含与(C)的解对同样的生成元对所对应的结点. 列出解来,表明没有这样的子图. 的确,甚至没有一条封闭的回路! 直到遇到一条回路,我们才需要把数对 a,b 和 $a\pm b$ 加以区分.

因此不知道有没有 4 个这样的平方数的例子. 两两相加有 5 个平方和的 4 个平方数的构造并不复杂.

A. R. Thatcher 把该问题与方程 $y^2=-x^8+35x^4-25$ 联系了起来. 仅有的整数解是 $(\pm1,\pm3)$,但是可能还有有限多个其他的有理解. 即使没有,这并不排除原来的问题有解.

差为平方数的 4 个平方数. 与上面(C)的延拓类似,这个问题

是对(M)的延拓. 一个顶点现在是五阶的,如果它与一个有 5 个结点或生成元对的圈相连接. 重要的是边的循环次序,而不是旋转的指向. (M)的一个解对应于三条顺序相连的边,这里我们必须把 α,β 和 $\alpha\pm\beta$ 区分开来:在图 11 中相应的结点用双线连接起来. 这种结点又是无穷阶的. 所要求的这种类型的四个平方数将对应于和 K_6 同胚的一个子图,它有 6 个顶点和 15 个结点,每条边上有一个结点. 到目前为止找到的仅有的圈标在图 11 中,它不是用作这个子图的一部分. 虽然不像有解,但是也不像有任何否定解的存在性的同余条件.

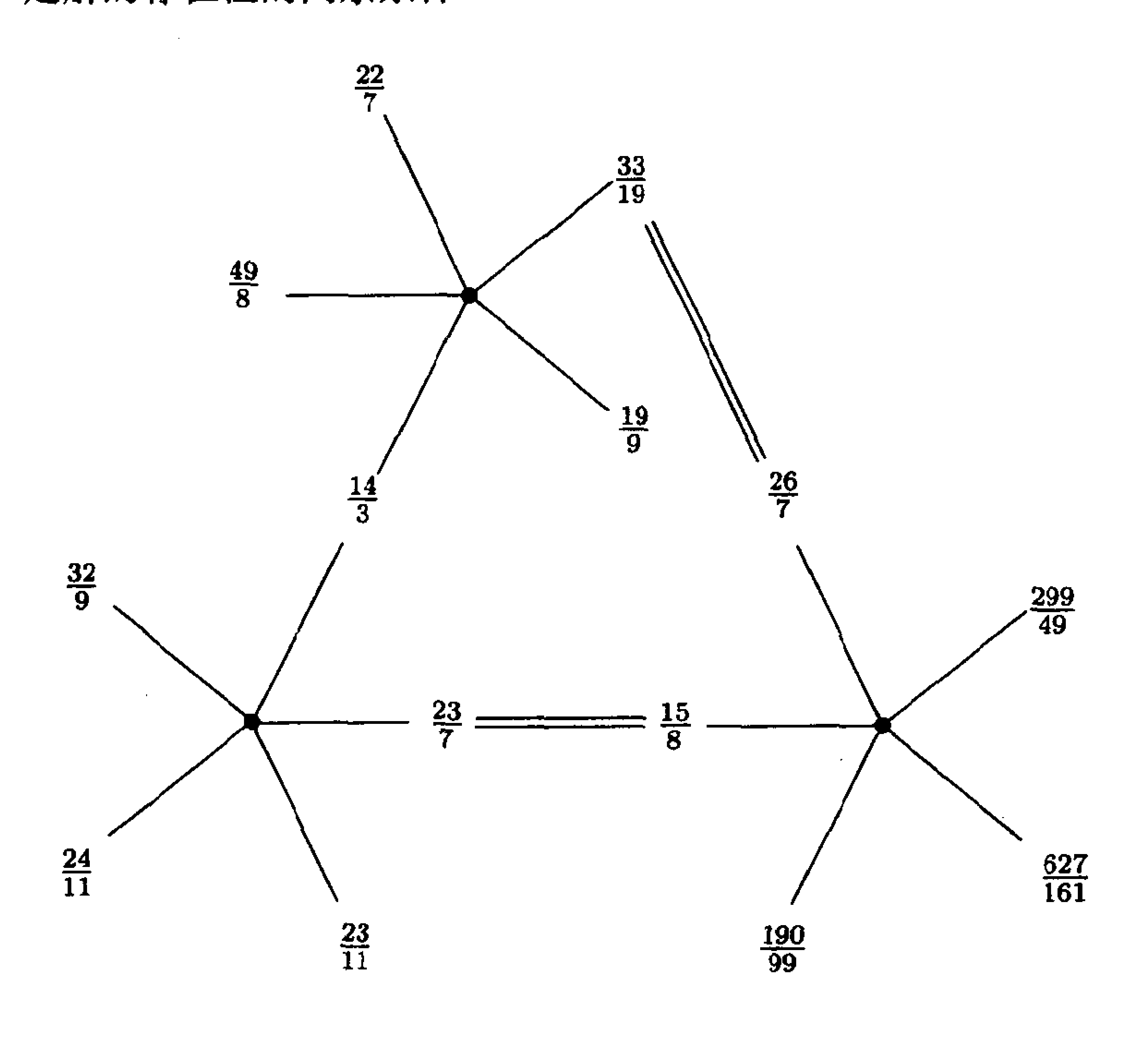


图 11　5 个生成元对的 3 个圈

尽管在生成元对 α,β 和 $\alpha\pm\beta$ 之间现在没有必然的联系,(M)的包含这两对生成元的解确实出现了. 这样一个解引导到 4

个平方数的序列,该序列中两个或3个相连的项之和全都是平方数. 这样一个序列能有多长? 对多于4的情形,我们需要(M)的解的一个5-圈的序列,每一个都包含相邻的生成元对 $\alpha,\beta;\overline{\alpha},\overline{\beta}$,这里 $\alpha\pm\beta,\overline{\alpha}\pm\overline{\beta}$ 的每一对都属于相邻的圈. Leech 找到了序列

(56,31)(17,6);(23,11)(23,7);(15,8)(26,7);

(33,19)(77,19);(48,29)(35,4);(39,31)(13,9),

这里 $23,11=17\pm6$ 等等,它给出八个这样的平方数的序列. 一个完全长方体的边的平方将会构成一个无穷(循环的)序列. 差全是平方数的四个非零平方数将引导出一个序列,它每隔三项的比值为常数:整数比将给出一个无穷序列. Leech 后来又给出一个"两端都惊人地小的"更长的序列

(14,1)(224,37);(261,187)(155,132);(287,23)(23,7);

(15,8)(26,7);(33,19)(77,19);(48,29)(35,4);(39,31)(13,9)

他问:"它们是否真的结束了?"他没有给出下述结论的证明:当 $(a+b,a-b)$ 不出现时,数对 (a,b) 不能出现. 他还有一些其他的有同样长度的序列,但到目前为止没有更长的了. Randall Rathbun 未能在(14,1)之前以及(13,9)之后加长这一序列,不过他通过在(56,31)的前面添上(26767,2185)(87,25)或(940,693)(87,25)而将原来的序列扩充成七项.

完全有理长方体. 在问题1,2,3的已知的数值解中,还没有解能给出一个完全长方体,许多参数解(例如(G))能证明得不到完全长方体. Spohn 用 Pocklington 的工作证明了(F)的两个互为导出长方体中有一个不是完全的,而 E. Z. Chein 和 Jean Lagrange 都证明了:导出长方体绝不是完全的. 另一方面,没有已知的参数解是完全的,所以仅由此不能证明完全长方体的不可能性. 上一节问题的一个解不一定给出完全长方体. Korec 证明了:完全有理长方体的最小的边必须超过 10^6. 深入的搜索(主要是由 Randall Rathbun 和 Torbjorn Granlund 做的)指出:完全有理长方体的所有的边必须都大于 333750000. 在搜索中,存储在未发表的数学表中的结果,即那3个问题的 $6800+6380+6749$ 个解被找到

了. 最近 Korec 证明了:(完全长方体的)最大的边大于 10^9. Leech 加强了 Horst Bergmann 的一个结果,由此证明了(完全长方体的)边、面对角线和体对角线的乘积必须被

$$2^8 \times 3^4 \times 5^3 \times 7 \times 11 \times 13 \times 17 \times 19 \times 29 \times 37$$

整除.

未解决的问题.(M) 的解有 3 个圈(它的图如图 12 所示)存在吗? 这里我们采用 John Leech 的写法:当其中同一对生成元属于两个圈时(如图 11 中的 14 和 3 这一对一样),就把边的比值写成分数,例如$\frac{y_1}{x_1}$;而在同一对生成元属于同一个圈、它们的和与差属于另一个圈的情形(如图 11 中的 15,8 以及 23,7),就把它写成一个比,例如 $x_2 : x_3$.

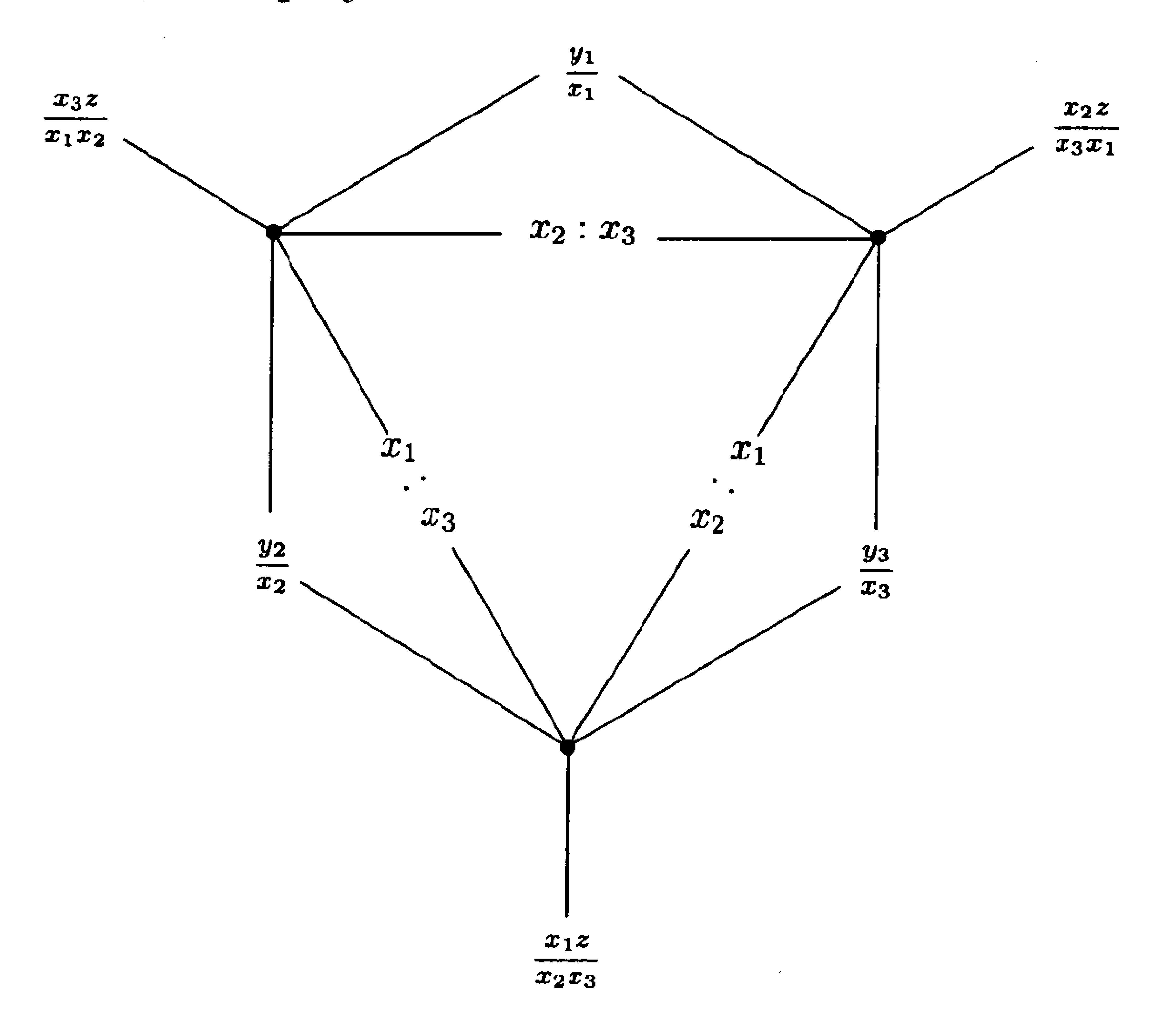


图 12 (M)的解有像这样的 3 个圈吗?

是否存在比值$(p^2-q^2)/2pq$，$(r^2+s^2)/2rs$，它们的积与商都有$(m^2-n^2)/2mn$的形式吗？

$$(a^2c^2-b^2d^2)(a^2d^2-b^2c^2)=(a^2b^2-c^2d^2)^2$$

有非平凡的解吗？这样一个解将产生出一个完全长方体．(M)的解有一个适合

$$\alpha_1/\beta_1=(p^2-q^2)/2pq,\quad \alpha_2/\beta_2=(r^2+s^2)/2rs$$

的5-圈吗？如果(C)的解作成的图中有回路出现的话，它会是什么样的回路呢？在(M)的解作成的图中会出现什么样的回路？(I)的解中有不同于(K)的圈存在吗？问题1中长方体的边的比值除了不能是3/4以外，还有什么样的边的比值不能出现？在问题3中呢？存在所有的边、所有的面对角线及体对角线都是有理数的平行六面体吗？Rathbun发现了41对本原的长方体，其中一个长方体的两条边等于另一个长方体的两条边．它们中的21个是问题1的解对，其体对角线是无理数；13个是问题2的解对；3个是问题3的解对，它有一条面对角线是无理数．有3个是问题1和3的解，而最后一个则是问题1和2的解．

参考文献

Andrew Bremner, Pythagorean triangles and a quartic surface, *J. reine angew. Math.*, **318**(1980) 120–125.

Andrew Bremner, The rational cuboid and a quartic surface, *Rocky Mountain J. Math.*, **18**(1988) 105–121.

T. Bromhead, On square sums of squares, *Math. Gaz.*, **44**(1960) 219–220; *MR* **23** #A1594.

Ezra Brown, $x^4+dx^2y^2+y^4$: some cases with only trivial solutions — and a solution Euler missed, *Glasgow Math. J.*, **31**(1989) 297–307; *MR* **91d**:11026.

W. Burnside, Note on the symmetric group, *Messenger of Math.*, **30**(1900–01) 148–153; *J'buch* **32**, 141–142.

E. Z. Chein, On the derived cuboid of an Eulerian triple, *Canad. Math. Bull.*, **20**(1977) 509–510; *MR* **57** #12375.

W. J. A. Colman, On certain semi-perfect cuboids, *Fibonacci Quart.*, **26** (1988) 54–57 (see also 338–343).

J. H. Conway & H. S. M. Coxeter, Triangulated polygons and frieze patterns, *Math. Gaz.*, **57**(1973) 87–94, 175–183 and refs. on pp. 93–94.

H. S. M. Coxeter, Frieze patterns, *Acta Arith.*, **18**(1971) 297–310; *MR* 44 #3980.

L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Diophantine Analysis, Washington, 1920: ch. 15, ref. 28, p. 448 and cross-refs. to pp. 446–458; ch. 19, refs 1–30, 40–45, pp. 497–502, 505–507.

Marcus Engel, Numerische Lösung eines Quaderproblems, *Wiss. Z. Pädagog. Hochsch. Erfurt/Mühlhausen Math.-Natur. Reihe*, **22**(1986) 78–86; *MR* **87m**: 11021.

P. W. Flood, *Math. Quest. Educ. Times*, **68**(1898), 53.

Martin Gardner, Mathematical Games, *Scientific Amer.*, **223**#1(Jul.1970) 118; correction, #3(Sep.1970)218.

W. Howard Joint, Cycles, Note 1767, *Math. Gaz.*, **28**(1944) 196–197.

Ivan Korec, Nonexistence of a small perfect rational cuboid, I., II., *Acta Math. Univ. Comenian.*, **42/43**(1983) 73–86, **44/45**(1984) 39–48; *MR* **85i**:11004, **86c**:11013.

Ivan Korec, Lower bounds for perfect rational cuboids, *Math. Slovaca*, **42** (1992) 565–582.

Maurice Kraitchik, On certain rational cuboids, *Scripta Math.*, **11**(1945) 317–326; *MR* **8**, 6.

Maurice Kraitchik, *Théorie des nombres*, t.3, Analyse Diophantine et applications aux cuboides rationnels, Paris, 1947.

Maurice Kraitchik, Sur les cuboides rationnels, in *Proc. Internat. Congr. Math.* 1954, Vol. 2, Amsterdam, 33–34.

Jean Lagrange, Sur le dérivé du cuboïde eulerien, *Canad. Math. Bull.*, **22** (1979) 239–241; *MR* **80h**:10022.

Jean Lagrange, Sets of n squares of which any $n-1$ have their sum square, *Math. Comput.*, **41**(1983) 675–681; *MR* **84j**:10012.

M. Lal & W. J. Blundon, Solutions of the Diophantine equations $x^2+y^2=l^2$, $y^2+z^2=m^2$, $z^2+x^2=n^2$, *Math. Comput.*, **20**(1966) 144–147; *MR* **32** #4082.

J. Leech, The location of four squares in an arithmetical progression with some applications, in *Computers in Number Theory*, Academic Press, London, 1971, 83–98; *MR* **47** #4913.

J. Leech, The rational cuboid revisited, *Amer. Math. Monthly*, **84**(1977) 518–533; corrections (Jean Lagrange) **85**(1978) 473; *MR* **58** #16492.

J. Leech, Five tables related to rational cuboids, *Math. Comput.*, **32**(1978) 657–659.

John Leech, A remark on rational cuboids, *Canad. Math. Bull.*, **24**(1981) 377–378; *MR* **83a**:10022.

John Leech, Four integers whose twelve quotients sum to zero, *Canad. J. Math.*, **38**(1986) 1261–1280; *MR* **88a**:11031; addendum 90-08-18.

R. C. Lyness, Cycles, Note 1581, *Math. Gaz.*, **26**(1942) 62; Note 1847, **29** (1945) 231–233; Note 2952, **45**(1961) 207–209.

"Mahatma", Problem 78, *The A.M.A.* [J. Assist. Masters Assoc. London] **44**(1949) 188; Solutions: J. Hancock, J. Peacock, N. A. Phillips, 225.

Eliakim Hastings Moore, The cross-ratio of $n!$ Cremona-transformations of order $n-3$ in flat space of $n-3$ dimensions, *Amer. J. Math.*, **30**(1900) 279–291; *J'buch* **31**, 655.

L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, *Proc. Cambridge Philos. Soc.*, **21**(1922) 179–192.
H. C. Pocklington, Some diophantine impossibilities, *Proc. Cambridge Philos. Soc.*, **17** (1914) 110–121, esp. p. 116.
Randall L. Rathbun, Table of equal area Pythagorean triangles, from coprimitive sets of integer generator pairs, iii+199pp. Deposited in UMT file; see *Math. Comput.*, **62**(1994) Review #11.
Randall L. Rathbun & Torbjorn Granlund, The classical rational cuboid table of Maurice Kraitchik, revised and enlarged, v(3pp. errata)+135pp. Deposited in UMT file; see *Math. Comput.*, **62**(1994) Review #10.
Randall L. Rathbun & Torbjorn Granlund, The integral cuboid table, with body, edge and face type of solutions, vii+399pp. (2 vols) + The integer cuboid auxiliary table, 100pp. Deposited in UMT file; see *Math. Comput.*, **62**(1994) Review #12.
W. W. Sawyer, Lyness's periodic sequence, Note 2951, *Math. Gaz.*, **45**(1961) 207.
Waclaw Sierpiński, Pythagorean Triangles, *Scripta Math. Studies*, **9**(1962), Yeshiva University, New York, Chap. 15, pp. 97–107.
W. Sierpiński, *A Selection of Problems in the Theory of Numbers*, Pergamon, Oxford, 1964, p. 112.
W. G. Spohn, On the integral cuboid, *Amer. Math. Monthly*, **79**(1972) 57–59; *MR* **46** #7158.
W. G. Spohn, On the derived cuboid, *Canad. Math. Bull.*, **17**(1974) 575–577; *MR* **51** #12693.

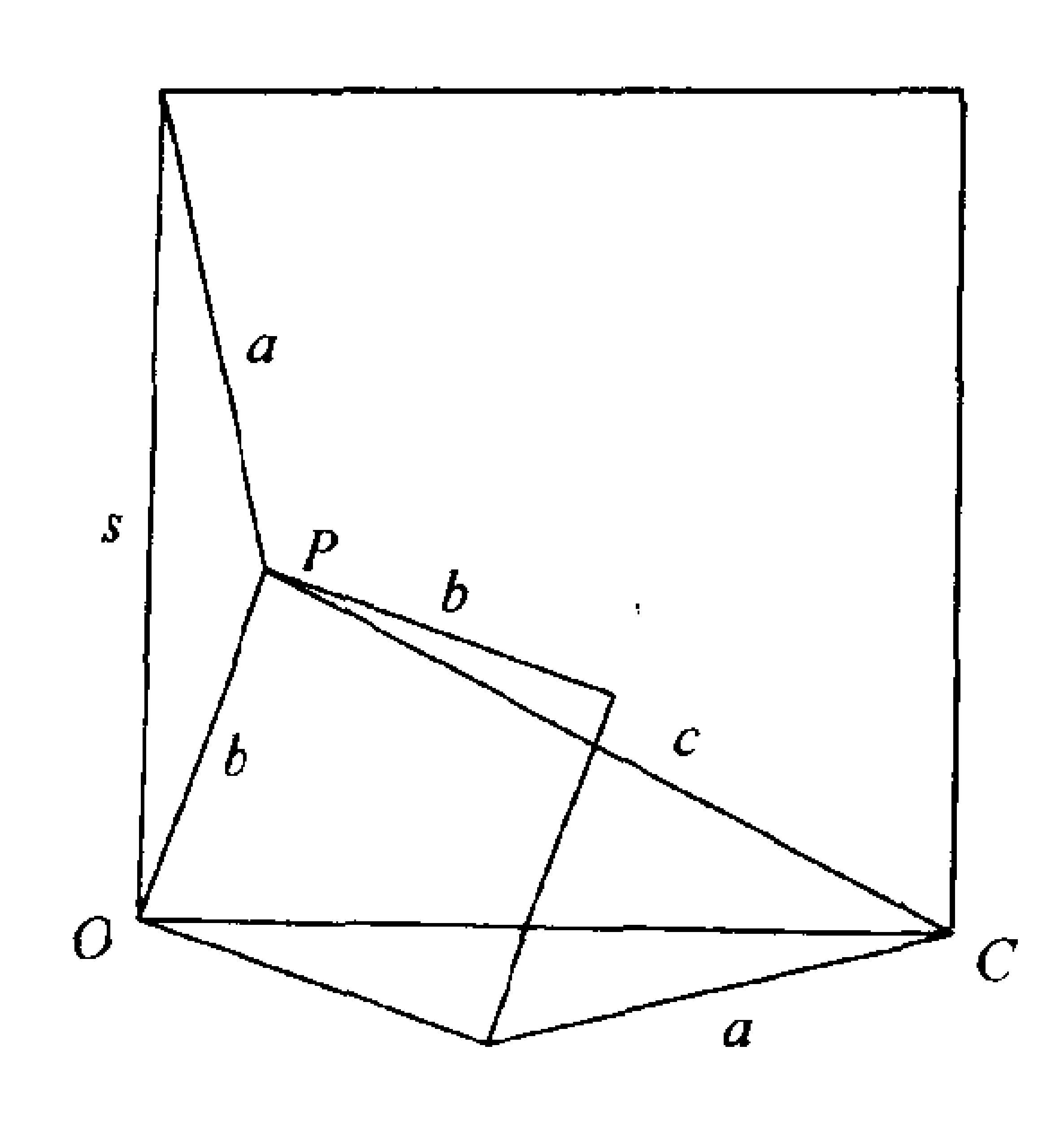
D19. 与正方形顶点的距离为有理数的点

存在一个点,它与单位正方形顶点的距离为有理数吗? 早先人们认为,可能不存在任何有这样 3 个有理距离的点的非平凡的例子(即点不在正方形的边上的例子),但是 John Conway 和 Mike Guy 发现了

$$(s^2 + b^2 - a^2)^2 + (s^2 + b^2 - c^2)^2 = (2bc)^2$$

的无穷多个整数解,这里 a,b,c 是一点与边长为 s 的正方形的 3 个顶点的距离. 这些解之间的关系画在图 13 上.

为使第四个距离 d 是一个整数,我们还需要 $a^2+c^2=b^2+d^2$. 在 3 个距离的问题中,s,a,b,c 中的一个可被 3 整除,一个可被 4 整除,一个可被 5 整除. 在 4 个距离的问题中,s 是 4 的倍数,而 a,b,c,d 是奇数(假设没有公因子). 如果 s 不是3(5)的倍数,那么 a,b,c,d 中有两个可以被 3(5)整除.



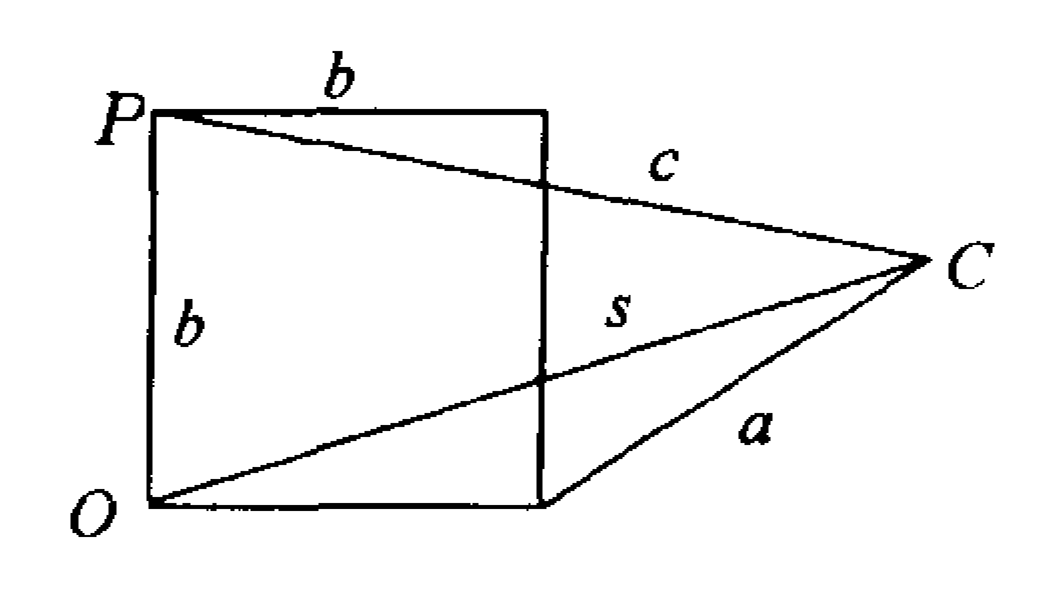


图 13　三距离问题的解及其逆问题

如果此问题推广到有理长方形，那么仍要求有 $a^2+c^2=b^2+d^2$. 这是 Martin Gardner 难题(Mathematical Games, *Sci. Amer.* 210 #6(June 1964), Problem 2, p. 116)的基础. 也见下面 Dodge 论文中的文献. 一个有关正方形的类似的问题(有一条无理边和一个无理距离)出现在 Dudeney 的 Canterbury Puzzles 一书中(见该书 No. 66, pp. 107～109, 212～213). Gardner 给出一份 Leslie J. Upton 和 J. A. H. Hunter 之间的通信的复印件. Hunter 在 1967 年 3 月 21 日的信中对在算术级数中的 3 个距离的问题给出无穷多个解：$a=m^2-2mn+2n^2$, $b=m^2+2n^2$, $c=m^2+2mn+2n^2$ 以及 $s^2=2m^2(m^2+4n^2)$. 这里，如果 $m=2(u^2+2uv-v^2)$, $n=u^2-2uv-v^2$, s 就是一个整数. 例如，与一个边长为 140 的正方形的 3 个相连的顶点有一个距离分别为 85, 99 和 113 的点. 可以证明：在这种解中，第四个距离绝不可能是有理数.

John Leech 找到了在平面上稠密的满足三距离问题的点. 它们包括 Conway-Guy 的解，以及 Hunter 的解(在图 13 的意义下)的“逆”. 但是还有其他的解，在某种意义上我们知道它们的“全部”. 考虑更一般的把一个有理正方形分割成有理三角形的问题. 已知至少要 4 个三角形，且恰有 4 个可供选择的安排：δ-构形，

κ-构形，ν-构形，χ-构形．头两个已经弄清楚是“对偶的”，其解由一族无限条椭圆曲线上的有理点给出．前面几百个由 Bremner 和 Guy 作了研究，他们也类似地处理了 ν-构形．然而 χ-构形，即“四距离”问题，仍是一个坚硬得令人惊讶、无法打开的坚果．

对应于与一个边长为 t 的等边三角形的顶点有整数距离 a，b，c 这一问题有无穷多个解．在每个解中，a,b,c,t 中有一个能被 3 整除，一个能被 5 整除，一个能被 7 整除，一个能被 8 整除．John Leech 对下述结论寄给我们一份精巧的初等证明：与任一个有有理边长的三角形的顶点相距有理距离的点在该三角形所在平面上是稠密的．这一结果早先曾由 Almering 证明过，见问题 D21 的文献．Arnfried Kemnitz 注意到：$a=m^2+n^2$，$b,c=m^2\pm mn+n^2$ 以及 $m=2(u^2-v^2)$，$n=u^2+4uv+v^2$ 给出 $t=8(u^2-v^2)(u^2+uv+v^2)$ 和无穷多个解，这些解中既没有点在三角形的边上，也没有点在该三角形的外接圆上．计算机搜索指出(57,65,73,112)是其中最小的解．

Thomas Berry 把最后列出的方程写成

$$2(s^4+b^4)+a^4+c^4=2(s^2+b^2)(a^2+c^2).$$

他还注意到，这一方程和与等边三角形对应的方程：

$$t^4+a^4+b^4+c^4=t^2a^2+t^2b^2+t^2c^2+b^2c^2+c^2a^2+a^2b^2$$

这两者都表示 Kummer 曲面(Kummer surface)，即恰有 16 个奇点的四次曲面．它们不是同构的，但有同样的特殊类型，称为**四面体**(tetrahedroid)．

我们有如下的推论：

- Kummer 曲面不是有理的：在“不存在能给出所有整数解(有理解)的多项式(有理函数)”这一意义上说，这两个问题都没有一般的参数解．

- 单参数的解族对应于曲面上可以参数化的曲线．例如，在等边三角形问题中，16 条二次曲线(它们在 Kummer 曲面上总是存在的)给出在三角形边上以及其外接圆周上的点．由 Arnfried Kemnitz 给出的解对应于平面截线 $b+c=2a$．

• 被 Bremner 和 Guy 用来寻找 δ-λ 构形的椭圆曲线在前面的曲面上作成一个曲线束,由于这两个曲面都是四面体,在"等边三角形"曲面上可能有一个椭圆曲线束,它允许类似的处理方法.

Berry 推广了 Almering 的结果,他证明了:如果一个三角形诸边上的正方形都是有理的,且此三角形至少有一边是有理的,那么与所有三个顶点相距有理距离的点的集合在该三角形所在平面上是稠密的.

Jerry Bergum 问:对什么样的整数 n,存在正整数 x,y, $x \perp y$, x 是偶数,使 $x^2+y^2=b^2$ 和 $x^2+(y-nx)^2=c^2$ 两者均为完全平方数?如果 $n=2m(2m^2+1)$,那么 $x=4m(4m^2+1)$, $y=mx+1$ 是一个解.如果 $n=\pm1,\pm2,\pm4,\pm11$,或 $\pm p$(这里 $p\equiv3 \bmod 4$,且 p^2+4 是一个素数,例如 $\pm3,\pm7$),那么它就没有解. Bergum 得到若干个无穷族的 n 的值,对于这些 n 的值问题有解,例如 $n=8t^2\pm4t+2(t>0)$.对 $n=\pm5,\pm6,\pm8,\pm9,\pm14,\pm19$,问题有解.如果 $n=8$,则使 y 存在的最小的 x 是 $x=2996760=2^3\cdot3\cdot5\cdot13\cdot17\cdot113$;如果 $n=19$,最小的 x 是 2410442371920. 从图 15(b)可以看出 $n=5$, $x=120$, $y=391$ 是一个解.这个问题和原来的问题的联系是:(x,y)是与原点 O 以及一个边长为 $s=nx$ 的正方形的一个相邻的顶点距离为 b 和 c 的点 P 的坐标,其中 n 是一个整数.

Ron Evans 注意到该问题可如下陈述:在整数边长的三角形中,什么样的整数 n 能作为底与高的比值出现? n 的符号取正还是取负,要看该三角形是锐角还是钝角三角形而定(例如 $n=-29$, $x=120$, $y=119$ 是一个解).他还问到与之对偶的问题:求出底能整除高的一切整数边长的三角形.这里高与底的比值 1 和 2 不可能出现,但是 3 可以(例如:底为 4;边长为 13,15;高为 12).如果一个比值能出现,是否存在无穷多个有此比值的本原三角形呢? K. R. S. Sastry 给出三角形(3389,21029,24360)和(26921,42041,68880),在每一个三角形中,底与高的比值都是 42,而(25,26,3)和(17,113,120)有比值 1/8 和 8(在每种情形,三数组的第

三个数都是该三角形的底).

参考文献

J. H. J. Almering, Rational quadrilaterals, *Nederl. Akad. Wetensch. Proc. Ser. A*, **66** = *Indagationes Math.*, **25**(1963) 192–199; II **68** = **27**(1965) 290–304; *MR* **26** #4963, **31** #3375.

T. G. Berry, Points at rational distance from the corners of a unit square, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.*(4), **17**(1990) 505–529; *MR* **92e**:11021.

T. G. Berry, Points at rational distances from the vertices of a triangle, *Acta Arith.*, **62**(1992) 391–398.

T. G. Berry, Triangle distance problems and Kummer surfaces, (to appear).

Andrew Bremner & Richard K. Guy, The delta-lambda configurations in tiling the square, *J. Number Theory*, **32**(1989) 263–280; *MR* **90g**:11031.

Andrew Bremner & Richard K. Guy, Nu-configurations in tiling the square, *Math. Comput.*, **59**(1992) 195–202, S1–S20; *MR* **93a**:11019.

Clayton W. Dodge, Problem 966, *Math. Mag.*, **49**(1976) 43; partial solution **50**(1977) 166–167; comment **59**(1986) 52.

R. B. Eggleton, Tiling the plane with triangles, *Discrete Math.*, **7**(1974) 53–65.

R. B. Eggleton, Where do all the triangles go? *Amer. Math. Monthly*, **82** (1975) 499–501.

Ronald Evans, Problem E2685, *Amer. Math. Monthly*, **84**(1977) 820.

N. J. Fine, On rational triangles, *Amer. Math. Monthly*, **83**(1976) 517–521.

Richard K. Guy, Tiling the square with rational triangles, in R. A. Mollin (ed.) Number Theory & Applications, *Proc. N.A.T.O. Adv. Study Inst., Banff 1988*, Kluwer, Dordrecht, 1989, 45-101.

W. H. Hudson, Kummer's Quartic Surface, reprinted with a foreword by W. Barth, Cambridge Univ. Press, 1990.

Arnfied Kemnitz, Rational quadrangles, Proc. 21st SE Conf. Combin. Graph Theory Comput., Boca Raton 1990, *Congr. Numer.*, **76**(1990) 193–199; *MR* **92k**:11034.

J. G. Mauldon, An impossible triangle, *Amer. Math. Monthly*, **86**(1979) 785–786.

C. Pomerance, On a tiling problem of R. B. Eggleton, *Discrete Math.*, **18** (1977) 63–70.

D20. 相距有理数的 6 个点

本书第一版曾问道:“平面上是否存在 6 个点,其中没有三点共线,也没有四点共圆,且它们相互间的距离都是有理数?”Leech 指出:这样的构形可以通过将 6 个边长和中线均为有理数的同样的三角形装配起来而得到. Euler 研究过这样的三角形(见 D21):最简单的边长为 68,85,87,而中线各是 158,131,127 的一半(图

14(a)). Harborth 和 Kemnitz 证明了:这个三角形导出相互距离为整数、无三点共线、无四点共圆的 6 个点的最小构形. 关于一个同心圆作反演,可得到一个相关的构形;此时它的 6 个三角形相似,但不再全等. 是否任何一个这样的构形都可以延拓? 是否有多于 6 个这样的点的集合? Kemnitz 展示了一个有整数距离(其中有 13 个距离是不同的,最大的一个距离是 319(图 14(b)))的 6 个点的不对称的集合.

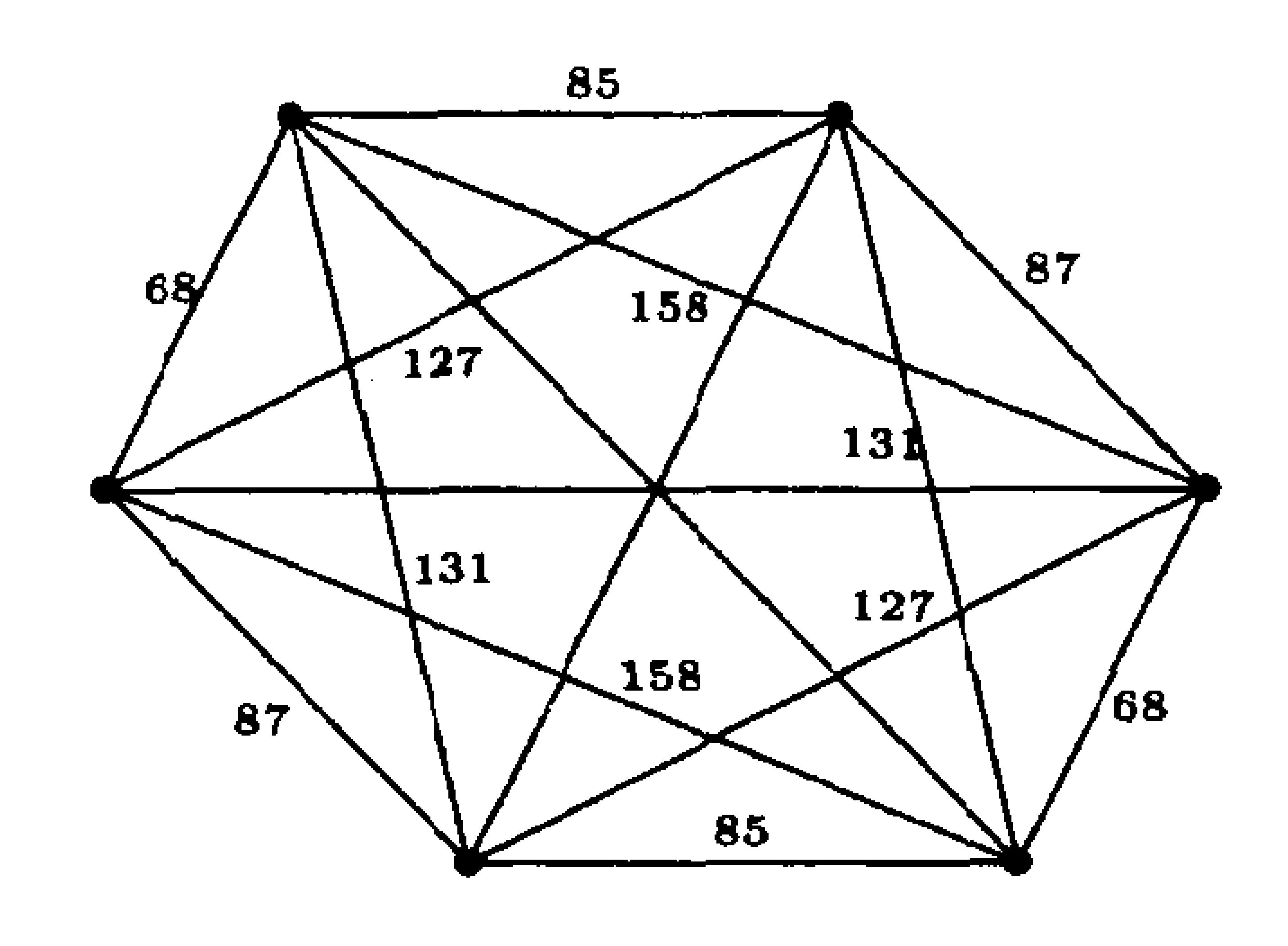


图 14(a) 一个有有理中线、关于形心对称的三角形

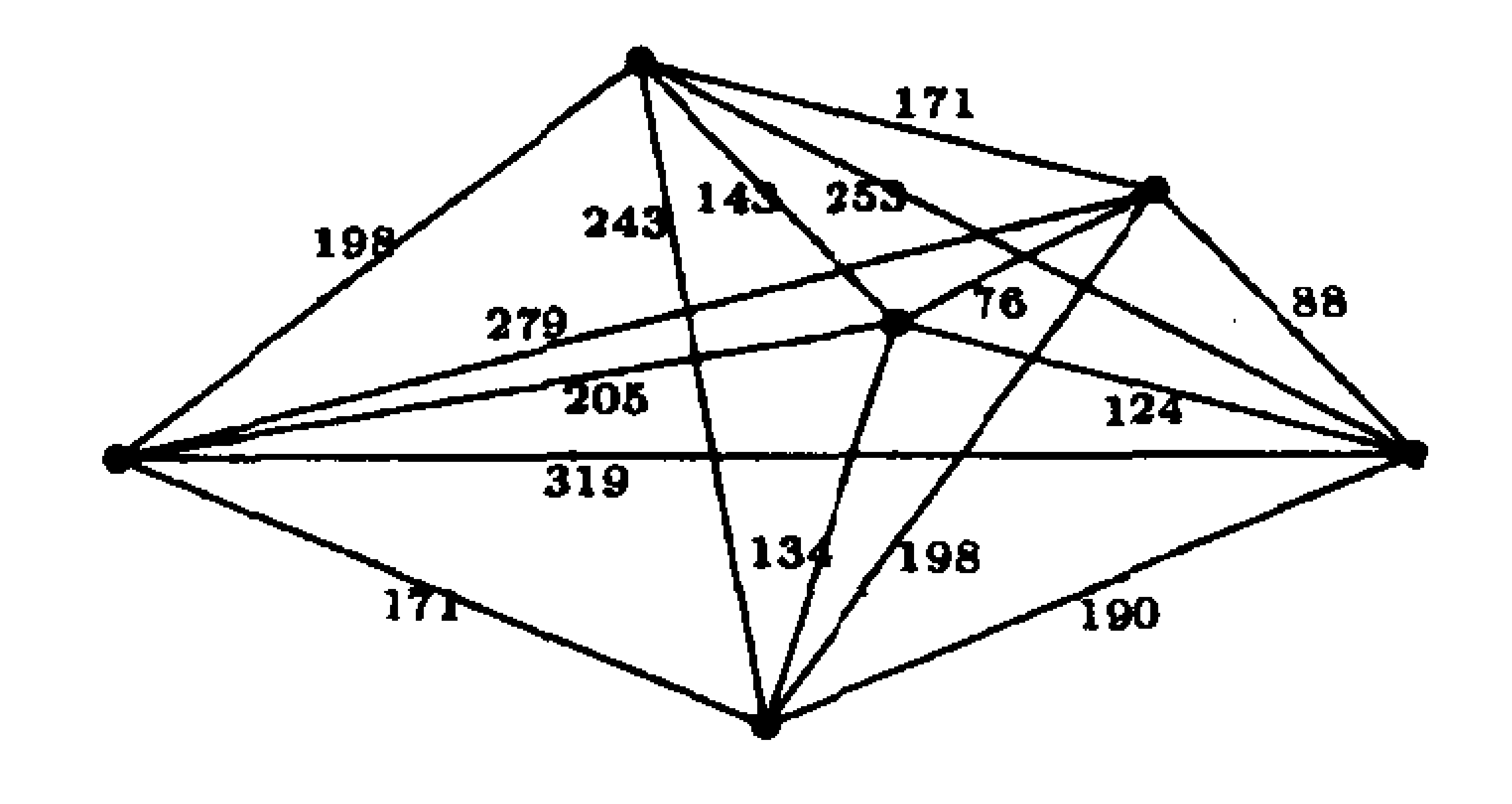


图 14(b) 有整数距离(其中 13 个距离是不同的)的 6 个点

有两个相反的极端的猜想:(a)存在一个固定的数 c,使得平面上任何 n 个相互距离是有理数的点都包含至少 $n-c$ 个共线或共圆的点;(b)(属于 Besicovitch,但是在 1959 年他对此又表示了

相反的意见)任何多边形都可以用边长和对角线均为有理数的多边形来任意精确地加以逼近. 如果(a)成立,c 的最大值是什么?

如果我们有一个无穷点列 $\{x_i\}$,其中所有点之间的距离都是有理数,我们能刻画它的极限点的集合吗? Euler 已知它们在圆周上可以是稠密的. 如果该点列在平面上稠密,Ulam 猜想不可能所有的距离都是有理数. 它是否包含一个稠密的子序列,其所有距离都是无理数呢?

我们可以选取一条直线和位于一条垂直直线上、离开它单位长距离的两个点;在第一条直线上离交点的距离形如 $(u^2-v^2)/2uv$ 的点构成一个无穷点集,其中所有两点间的距离均为有理数. 关于一个圆心在直线外的一点的圆作反演,我们得到圆周上一个稠密点集及其圆心,它们两两的距离都是有理数. 这就对圆内接多边形证明了猜想(b). Peeples(他提到 Huff)将这推广到一条直线,在它的一条垂直线上有 4 个点与该直线的距离分别为 $\pm p$, $\pm q$. 如果 q/p 可以表为两个不同的形如 $(u^2-v^2)/2uv$ 的比值的乘积,那么它就有无穷多种这样的表示,且在第一条直线上就有无穷多个点,这些点两两的距离以及它们和那 4 个直线外的点之间的距离都是有理数. 于是猜想(a)中 c 至少是 4. 关于一个圆心在直线外的那 4 个点中的一点的圆作反演,我们得到在一个圆周上稠密的点集,加上它的圆心以及一对关于该圆对称的点,所有这些点之间都有有理距离. 于是对猜想(a)中的圆来说,常数 c 至少是 3. 它们是 c 对无穷多个集合的最大值吗?

什么样的有限集会超过 c 的这些值呢? Leech 给出无穷多族 9 个点的集合,其中没有多于 4 点共线或共圆,从而对这些集合有 $c=5$. 它们基于联立不定方程

$$x^2+y^2=\square,$$
$$x^2+z^2=\square,$$
$$x^2+(y+z)^2=\square,$$
$$x^2+(y-z)^2=\square$$

的解;最简单有 $x=120, y=209, z=182$(图 15(b)).

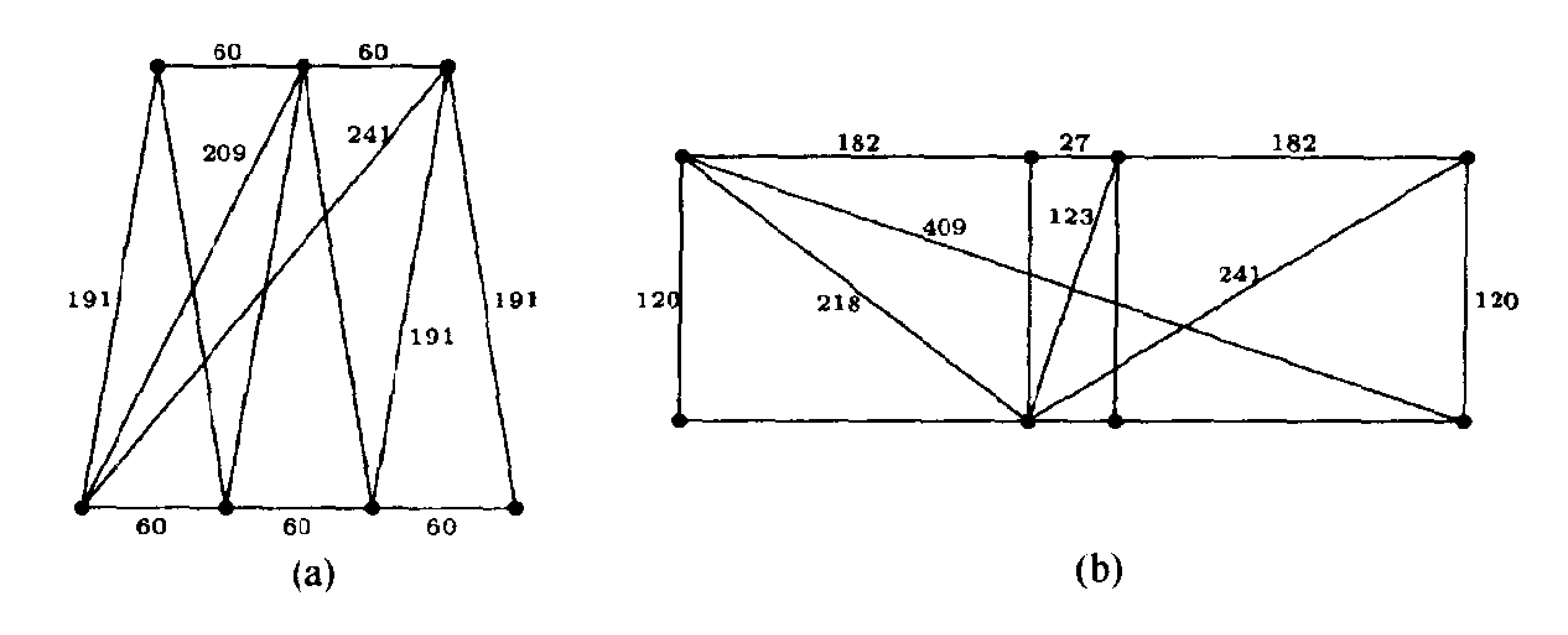


图 15　Leech 所作的有有理距离的点的构形

Lagrange 和 Leech 给出了无穷族由整数 a_1, a_2, a_3 和 b_1, b_2, b_3 组成的三数组对，使 9 个和 $a_i^2 + b_j^2$ 都是平方数．这些引导出在两条互相垂直的直线上的 13 个点的集合，其中包括它们的交点、在一条直线上的点 $(\pm a_i, 0)$ 和在另一条直线上的点 $(0, \pm b_j)$，每两点之间的距离皆为有理数，且无多于 7 点共线或多于 4 点共圆，从而对这些集合有 $c = 6$．最简单的例子有 $a_i = 952, 1800, 3536$ 以及 $b_j = 960, 1785, 6630$．他们还找到一个其中的三数组可以推广成四数组的例子，它有

$$a_i = 9282000,\quad 26822600,\quad 60386040,$$

$$b_j = 7422030,\quad 8947575,\quad 22276800,\quad 44142336,$$

但这些仍然只能给出 $c = 6$．Leech 后来又找到 3 个进一步的例子．能找到一对四数组，使所有 16 个和 $a_i^2 + b_j^2$ 都是平方数吗？如果行的话，我们就可以得到一个有 17 个点且相互有整数距离的集合，使 $c = 8$．

Noll 和 Bell 寻找无三点共线、无四点共圆的构形，不过他们只用格点．他们把这样的构形称为 N-群集（N-clusters）．他们与 William Kalsow 和 Bryan Rosenberg 独立地发现了 6-群集 (0,0)，(132, − 720)，(546, − 272)，(960, − 720)，(1155, 540)，(546, 1120)．他们定义一个 N-群集的广延（extent）是圆心在其中一个点且包含所有这些点的最小的圆的半径．他们找到了91个广延

小于 20937 的不等价的素 6-群集,但没有找到 7-群集.

参考文献

M. Altwegg, Ein Satz über Mengen von Punkten mit ganzzahliger Entfernung, *Elem. Math.*, **7**(1952) 56–58.

D. D. Ang, D. E. Daykin & T. K. Sheng, On Schoenberg's rational polygon problem, *J. Austral. Math. Soc.*, **9**(1969) 337–344; *MR* **39** #6816.

A. S. Besicovitch, Rational polygons, *Mathematika*, **6**(1959) 98; *MR* **22** #1557.

D. E. Daykin, Rational polygons, *Mathematika*, **10**(1963) 125–131; *MR* **30** #63.

D. E. Daykin, Rational triangles and parallelograms, *Math. Mag.*, **38**(1965) 46–47.

H. Harborth, On the problem of P. Erdős concerning points with integral distances, *Annals New York Acad. Sci.*, **175**(1970) 206–207.

H. Harborth, Antwort auf eine Frage von P. Erdős nach fünf Punkten mit ganzzahligen Abständen, *Elem. Math.*, **26**(1971) 112–113.

H. Harborth & A. Kemnitz, Diameters of integral point sets, *Intuitive geometry (Siófok, 1985)*, *Colloq. Math. Soc. János Bolyai*, **48**(1987) 255–266, North-Holland, Amsterdam-New York; *MR* **88k**:52011.

G. B. Huff, Diophantine problems in geometry and elliptic ternary forms, *Duke Math. J.*, **15**(1948) 443–453.

A. Kemnitz, Integral drawings of the complete graph K_6, in Bodendiek & Henn, *Topics in Combinatorics and Graph Theory, Essays in honour of Gerhard Ringel*, Physica-Verlag, Heidelberg, 1990, 421–429.

Jean Lagrange, Points du plan dont les distances mutuelles sont rationnelles, *Séminaire de Théorie des Nombres de Bordeaux*, 1982-1983, Exposé no. 27, Talence 1983.

Jean Lagrange, Sur une quadruple équation. *Analytic and elementary number theory* (Marseille, 1983), 107–113, *Publ. Math. Orsay*, 86-1, *Univ. Paris XI, Orsay*, 1986; *MR* **87g**:11036.

Jean Lagrange & John Leech, Two triads of squares, *Math. Comput.*, **46** (1986) 751–758; *MR* **87d**: 11018.

John Leech, Two diophantine birds with one stone, *Bull. London Math. Soc.*, **13**(1981) 561–563; *MR* **82k**:10017.

D. N. Lehmer, Rational triangles, *Annals Math. Ser. 2*, **1**(1899–1900) 97–102.

L. J. Mordell, Rational quadrilaterals, *J. London Math. Soc.*, **35**(1960) 277–282; *MR* **23** #A1593.

L. C. Noll & D. I. Bell, n-clusters for $1 < n < 7$, *Math. Comput.*, **53** (1989) 439–444.

W. D. Peeples, Elliptic curves and rational distance sets, *Proc. Amer. Math. Soc.*, **5**(1954) 29–33; *MR* **15** 645f.

T. K. Sheng, Rational polygons, *J. Austral. Math. Soc.*, **6**(1966) 452–459; *MR* **35** #137.

T. K. Sheng & D. E. Daykin, On approximating polygons by rational polygons, *Math. Mag.*, **38**(1966) 299–300; *MR* **34** #7463.

D21. 有整数边长、整数中线长和整数面积的三角形

存在有整数边长、整数中线长和整数面积的三角形吗？文献中有关于不可能性的不正确的"证明"，但该问题依然未得到解决. 对于那些自诩为解决了此问题的人来说，找出在 Schubert 和 Eggleston 的讨论中的错误（参考下面），或许是颇有教益的. 有一个时候人们曾经怀疑在一个 Heron 三角形（指边长和面积均为整数的三角形——译者注）中甚至不可能有两条有理中线，但是 Randall L. Rathbun, Arnfried Kemnitz 和 R. H. Buchholz 的发现表明：它们能存在. 最近，Rathbun 发现了无穷多个这种三角形，因而看起来猜想有无穷多个无穷族存在是合理的，但这与有三条有理中线的三角形的存在性及不可能性问题一样，仍然未获得证明. 如果我们不要求面积是有理数，就可以有许多解. Euler 给出了一个五次的参数解

$$a = 6\lambda^4 + 20\lambda^2 - 18,$$
$$b, c = \lambda^5 \pm \lambda^4 - 6\lambda^3 \pm 26\lambda^2 + 9\lambda \pm 9,$$

它的中线为

$$-2\lambda^5 + 20\lambda^3 + 54\lambda,$$
$$\pm \lambda^5 + 3\lambda^4 \pm 26\lambda^3 - 18\lambda^2 \pm 9\lambda + 27.$$

最近 George Cole 证明了：不计对称性，恰只有两个五次的参数解，即 Euler 的一个解和一个新的参数解. 到目前为止这些结果尚未产生出有有理面积的非退化的三角形.

由毕达哥拉斯三角形提出了一大堆问题. Eckert 问：是否有两个不同的毕达哥拉斯三角形，它们边长的乘积相等？即

$$xy(x^4 - y^4) = zw(z^4 - w^4)$$

是否有非零整数解？Prothro 问：是否可能一个乘积是另一个的两倍？更一般地，Leech 问：两个这样的乘积的比值能是怎样小的整数？当 $x, y = z \pm w$ 时，平凡地有 $xy(x^4 - y^4) = 8zw(z^4 - w^4)$.

既然每个乘积都能被 3·4·5 整除,从 $13=\frac{5\cdot12\cdot13}{3\cdot4\cdot5}$向上的许多整数也都是可能的. 更妙的是 $11=\frac{21\cdot220\cdot221}{13\cdot84\cdot85}$,更为复杂地有

$$6=\frac{6^3\cdot24\cdot143\cdot145}{135\cdot352\cdot377}.$$

它们是最小的吗?

他还注意到:令 $x,y=z\pm w$,则一个乘积是另一个的 8 倍.

有多少个本原的毕达哥拉斯三角形能有同样的面积? Charles L. Shedd 在 1945 年发现了一组 3 个这样的三角形,它们的生成元分别是(77,38),(78,55)和(138,5). 1986 年 Rathbun 又找到三组这样的三角形组:

(1610,869),(2002,1817),(2622,143);

(2035,266),(3306,61),(3422,55);

(2201,1166),(2438,2035),(3565,198)

第五组三角形(7238,2465),(9077,1122),(10434,731)是在接下来的那些日子里由 Dan Hoey 和 Rathbun 相互独立地发现的. 有无穷多个这样的三数组吗? 有四个三角形一组的吗?

Sastry 要求这样的毕达哥拉斯三角形:它的两直角边长是一个平方数和一个三角数,而斜边长则是一个五角形数$\frac{1}{2}n(3n-1)$. 除了(3,4,5)和(105,100,145)以外,是否还有任何非平凡的例子呢? 如果允许取负秩的五角形数$\frac{1}{2}n(3n+1)$,这会对问题的解有帮助吗?

由于对解有理盒子的问题感到失望(D18),有些人研究了其他有整数距离的多面体. 例如,有 7 个拓扑上不同的凸六面体,它的有整数距离的例子由 Harborth 和 Kemnitz(见 D20)以及由 Peterson 和 Jordan 所发现. Sastry 要求有理盒子问题的解,但在问题中用三角数代替了平方数. Charles Ashbacher 给出三角数 66,105,105,它们两两的和以及全部的和都是三角数.

参考文献

J. H. J. Almering, Heron problems, thesis, Amsterdam, 1950.

Ralph Heiner Buchholz, On triangles with rational altitudes, angle bisectors or medians, PhD thesis, Univ. of Newcastle, Australia, 1989.

George Raymond Cole, Triangles all of whose sides and medians are rational, PhD dissertation, Arizona State University, May 1991.

Ernest J. Eckert, Problem 994, *Crux Mathematicorum*, **10**(1984) 318; comment **12**(1986) 109.

H. G. Eggleston, A proof that there is no triangle the magnitudes of whose sides, area and medians are integers, Note 2204, *Math. Gaz.*, **35**(1951) 114–115.

H. G. Eggleston, Isosceles triangles with integral sides and two integral medians, Note 2347, *Math. Gaz.*, **37**(1953) 208–209.

Albert Fässler, Multiple Pythagorean number triples, *Amer. Math. Monthly*, **98**(1991) 505–517; *MR* **92d**:11021.

Martin Gardner, Mathematical Games: Simple proofs of the Pythagorean theorem, and sundry other matters, *Sci. Amer.* **211#4** (Oct. 1964) 118–126.

Blake E. Peterson, Integer polyhedra, Ph.D. dissertation, Washington State University, 1993.

Blake E. Peterson & James H. Jordan, Integer polyhedra and the perfect box, (preprint, 93-01-08).

Blake E. Peterson & James H. Jordan, Integer hexahedra equivalent to perfect boxes, *Amer. Math. Monthly*, **101**(1994).

E. T. Prothro, *Amer. Math. Monthly* **95**(1988) 31.

Randall L. Rathbun, Letter to the Editor, *Amer. Math. Monthly*, **99**(1992) 283–284.

K. R. S. Sastry, Problem 1725, *Crux Mathematicorum*, **18**(1992) 75.

K. R. S. Sastry, Problem 1832, *Crux Mathematicorum*, **19**(1993) 112.

H. Schubert, *Die Ganzzahligkeit in der algebraischen Geometrie*, Leipzig, 1905, 1–16.

D22. 具有有理容度的单纯形

存在任何维数的单纯形，它所有的容度(长度、面积、体积、超体积)都是有理数吗？在 2 维的情形，答案是肯定的：存在无穷多个 Heron 三角形(Heron triangle)，它们有有理边长和有理面积．一个例子是边长 13，14，15 的三角形，它有面积 84．在 3 维的情形，答案仍然是肯定的，但是所有的四面体能用这样的有理四面体来任意逼近吗？

John Leech 注意到：4 个一模一样的锐角 Heron 三角形组装

在一起就构成这样一个四面体，只要它的体积是有理数即可，而做到这一点并不困难．例如，取三对长度分别为 148，195，203 的对棱．这是最小的例子：他发现后面几个三数组是

$$(533,875,888),\ (1183,1479,1804),$$
$$(2175,2296,2431),\ (1825,2748,2873),$$
$$(2180,2639,3111),\ (1887,5215,5512),$$
$$(6409,6625,8484),\ (8619,10136,11275).$$

他还提出查验 Dickson 的数论史一书第二卷 p. 224 上的下列参考文献[A17]：

R. Güntsche, *Sitzungsber. Berlin Math. Gesell.*, **6**(1907) 38–53.

R. Güntsche, *Archiv Math. Phys.*(3), **11**(1907) 371.

E. Haentzschel, *Sitzungsber. Berlin Math. Gesell.*, **12**(1913) 101–108 & **17**(1918) 37–39 (& *cf.* **14**(1915) 371).

O. Schultz, Ueber Tetraeder mit rationalen Masszahlen der Kantenlängen und des Volumen, Halle, 1914, 292 pp.

Dickson 要求得到最后这篇文章的复印件．他得到了吗？有谁知道它的复印件？其所有者愿意将它捐赠还是出售给 Strens 收藏馆（Strens 收藏馆是位于 Calgary 大学内的一个数学书收藏馆——译者注）呢？

Leech 也注意到，根据 D18 中问题 3（求一个盒子，它除了一条面对角线以外，其余距离皆为有理数）的解，在 3 维的情形这个问题有肯定的答案．这个问题曾经作为第 930 个问题发表在 *Crux Mathematicorum*，10（1984）#3，p. 89 上，由 COPS（也许这是 Carleton (Ottawa) Problem Solvers 的字头作成的笔名）给出的解是：

取一个四面体，它有三条相互垂直的棱

$$a = p^2q^2 - r^2s^2,\quad b = 2pqrs,\quad c = p^2r^2 - q^2s^2.$$

那么 a^2+b^2, b^2+c^2 是平方数，且如果

$$p^4 + s^4 = q^4 + r^4,$$

那么 $a^2+b^2+c^2=(p^4+s^4)(q^4+r^4)$ 是平方数．（John Leech 注意到除此而外的其他情形，并给出 4 个意外的例子：

$$(1^4 + 2^4)(2^4 + 13^4) = 697^2,$$

$$(1^4+2^4)(38^4+43^4) = 9673^2,$$
$$(1^4+2^4)(314^4+863^4) = 1275643^2,$$
$$(1^4+3^4)(9^4+437^4) = 1729298^2.$$
它们蕴含形如$(2^4+13^4)(38^4+43^4)$的进一步的例子.)

这个方程由 Euler 所解决. D9 中提到的解是:

$$p,q = x^7+x^5y^2-2x^3y^4 \pm 3x^2y^5+xy^6$$
$$r,s = x^6y \pm 3x^5y^2-2x^4y^3+x^2y^5+y^7,$$

但这并非在任何意义下都是完全的.

Buchholz 发现棱的长度≤156 的惟一的有理四面体是:棱长 117,80,53,52,51,84,面的面积 1800,1890,2016,1170 以及体积 18144. 他还证明了:仅当 d 形如$4k(k+1)$或 $2k^2-1$ 时,有有理棱长的正则维数的单纯形就有有理的 d 维体积.

Dove 和 Sumner 将"四面体的面有有理面积"这一条件放宽,他找到体积为 3 的两个四面体,它们的对棱长各为(32,76)(33,70)(35,44)和(21,58)(32,76)(47,56). 他们问:是否有无穷多个四面体,他们都有整数棱长和同样的整数体积? 是否有这样的四面体,它的体积是 3 的任何给定的整数倍? 除了 87 以外,对从 3 到 99 他们都找到了这样的例子.

Sierpiński 和 Leitmann 提到过一个四面体,它有一对对棱是 896 和 990,另外四条棱都是 1073,有两个面的面积是 436800 和 471240,而体积是 62092800.

参 考 文 献

Ralph Heiner Buchholz, Perfect pyramids, *Bull. Austral. Math. Soc.*, **45**(1991) 353–368.

Kevin L. Dove & John L. Sumner, Tetrahedra with integer edges and integer volume, *Math. Mag.*, **65**(1992) 104–111.

K. È. Kalyamanova, Rational tetrahedra (Russian), *Izv. Vyssh. Uchebn. Zaved. Mat.*, **1990** 73–75; *MR* **92b**:11014.

W. Lietzmann, Der pythagoreisch Lehrsatz, Leipzig, 1965, p. 91 [not in 1930 edition].

W. Sierpiński, *Pythagorean Triangles*, New York, 1962, p. 107.

D23. 某些四次方程

在许多未解决的不定方程中的又一个方程是

$$(x^2-1)(y^2-1)=(z^2-1)^2,$$

尽管 Schinzel 和 Sierpiński 曾找到了它所有的适合 $x-y=2z$ 的解. 曹珍富(Cao Zhen-Fu)证明了:对 $l\leqslant 30$ 的其他值,此方程满足 $x-y=lz$ 的仅有的解是 $|x|=|y|$ 或 $|z|=1$. 王彦斌(Wang Yan Bin)证明了:这些是适合 $x-y=z^2+1$ 的仅有的解.

Kashihara 证明了:

$$(x^2-1)(y^2-1)=(z^2-1)$$

的所有解可以从平凡解$(n,1,1)$和$(1,n,1)$得出.

对方程 $x^2-1=y^2(z^2-1)$,Mignotte 证明了:如果 z 很大,那么 y 的最大素因子小于 $c\ln\ln y$.

Ron Graham 注意到,不定方程

$$2x^2(x^2-1)=3(y^2-1) \quad 和 \quad (2x-1)^2=2^n-7$$

中的每一个都有解 $x=0,1,2,3,6$ 和 91. 这是否仅仅是强小数法则的一个例子呢? 显然如此! 在一篇即将发表的论文中,Stroeker 和 Weger 发现 Graham 的方程有一对解$(0,\pm y)$以及 5 个四元解组$(\pm x,\pm y)$. 他们注意到:把 Ramanujan-Nagell 方程的解 $x=0$ 和 $x=1$ 分开来加以统计,而“忘掉了”解 $x=-1,-2,-5,-90$,这是不公正的.

Baragar 证明了:Katayama 研究过的方程

$$x(x+1)y(y+1)=z(z+1)$$

等价于 Markoff 型方程(见 D12)

$$x^2+y^2+z^2=2xyz+5,$$

并且他还计算了该方程小于 N 的解的个数.

参考文献

Cao Zhen-Fu, A generalization of the Schinzel-Sierpiński system of equations (Chinese; English summary), *J. Harbin Inst. Tech.*, **23**(1991) 9–14; *MR* **93b**:11026.

Kenji Kashihara, The Diophantine equation $x^2-1=(y^2-1)(z^2-1)$ (Japanese; English summary), *Res. Rep. Anan College Tech. No.* **26**(1990) 119–130; *MR* **91d**:11025.

Shin-ichi Katayama & Kenji Kashihara, On the structure of the integer solutions of $z^2=(x^2-1)(y^2-1)-a$, *J. Math. Tokushima Univ.*, **24**(1990) 1–11; *MR* **93c**:11013.

Maurice Mignotte, A note on the equation $x^2-1=y^2(z^2-1)$, *C. R. Math. Rep. Acad. Sci. Canada*, **13**(1991) 157–160; *MR* **92j**:11026.

A. Schinzel & W. Sierpiński, Sur l'equation diophantienne $(x^2-1)(y^2-1)=[((y-x)/2)^2-1]^2$, *Elem. Math.*, **18**(1963) 132–133; *MR* **29** #1180.

Wang Yan-Bin, On the Diophantine equation $(x^2-1)(y^2-1)=(z^2-1)^2$ (Chinese, English summary), *Heilongjiang Daxue Ziran Kexue Xuebao*, **1989** *no.* 4 84–85; *MR* **91e**:11028.

D24. 和、积相等的数组

对 $k>2$,方程 $a_1a_2\cdots a_k=a_1+a_2+\cdots+a_k$ 有解 $a_1=2,a_2=k,a_3=a_4=\cdots=a_k=1$. Schinzel 证明了:对 $k=6$ 或 $k=24$,它没有其他的解了. Misiurewicz 证明了:在 $k<1000$ 以内,$k=2,3,4,6,24,114$ 是使得该方程恰有惟一解的仅有的 k 值.

这个问题似乎首先是由 Trost 提出的,他的问题是要求方程 $a_1a_2\cdots a_k=a_1+a_2+\cdots+a_k=1$ 的有理解. 对 $k=3$ 它属于 Sierpiński;对 $k>3$ 属于 Schinzel. 在 *Amer. Math. Monthly* 的编辑评论中将这一结果推广到了 $k\leqslant10000$,而 M. L. Brown 对 k 给出了必要且充分条件,并将搜索范围扩大到了 $k\leqslant50000$.

参考文献

M. L. Brown, On the diophantine equation $\sum X_i=\prod X_i$, *Math. Comput.*, **42**(1984) 239–240; *MR* **85d**:11030.

M. Misiurewicz, Ungelöste Probleme, *Elem. Math.*, **21**(1966) 90.

E. P. Starke & others, Solution to Problem E2262 [1970, 1008] & editorial com-

ment, *Amer. Math. Monthly*, **78**(1971) 1021–1022.
E. Trost, Ungelöste Probleme, Nr. **14**, *Elem. Math.*, **11**(1956) 134–135.

D25. 包含 n 的阶乘的方程

$n!+1=x^2$ 的仅有的解是由 $n=4,5$ 和 7 给出的吗? Overholt 将此问题与 Szpiro 的一个猜想联系了起来. Erdös 和 Obláth 处理了方程 $n!=x^p\pm y^p(x\perp y,p>2)$. 对 $p=2$ 以及带正号的情形见 Leech 在 D2 所作的评论;对取负号的情形,把 $n!$ 分成两个偶数因子: $4!=5^2-1^2=7^2-5^2$, $5!=11^2-1^2=13^2-7^2=17^2-13^2=31^2-29^2$. 其解数是 $\frac{1}{2}d(n!/4)$.

Simmons 注意到对 $(m,n)=(2,3),(3,4),(5,5)$ 和 $(9,6)$ 有 $n!=(m-1)m(m+1)$,他问是否还有其他的解? 更一般地,他问道:是否有 $n!+x=x^k$ 的任何其他的解? 这是寻求用一种非平凡的方式将 $n!$ 分成 k 个连续整数的乘积这一问题的变种($k\neq n+1-j!$). 请与 B23 比较.

在一封 1993 年 5 月 7 日写给 Ron Graham 的信中, Nobuhisa Abe 说道:对 $k=5$,方程 $x(x+1)\cdots(x+k)=y^2-1$ 有惟一解 $(x,y)=(2,71)$,而对 $k=7$ 或 11 它没有解.

Berend 和 Osgood 证明了:如果 $P(x)$ 是一个次数 $\geqslant 2$ 的整系数多项式,那么使方程 $P(x)=n!$ 有整数解 x 的那种 n 的集合之密度为零.

参考文献

Daniel Berend & Charles F. Osgood, On the equation $P(x)=n!$ and a question of Erdős, *J. Number Theory*, **42**(1992) 189–193; *MR* **93e**:11016.
B. Brindza & P. Erdős, On some Diophantine problems involving powers and factorials, *J. Austral. Math. Soc. Ser. A* **51**(1991) 1–7; *MR* **92i**:11036.
H. Brocard, Question 1532, *Nouv. Corresp. Math.*, **2**(1876) 287; *Nouv. Ann. Math.*(3) **4**(1885) 391.
P. Erdős & R. Obláth, Über diophantische Gleichungen der Form $n!=x^p\pm y^p$ und $n!\pm m!=x^p$, *Acta Szeged*, **8**(1937) 241–255.
M. Kraitchik, Recherches sur la Théorie des Nombres, tome 1, Gauthier-Villars,

Paris, 1924, 38–41.
Marius Overholt, The Diophantine equation $n! + 1 = m^2$, *Bull. London Math. Soc.*, **25**(1993) 104; *MR* **93m**:11026.
Richard M. Pollack & Harold N. Shapiro, The next to last case of a factorial diophantine equation, *Comm. Pure Appl. Math.*, **26**(1973) 313–325; *MR* **50** #12915.
Gustavus J. Simmons, A factorial conjecture, *J. Recreational Math.*, **1**(1968) 38.

D26. 各种类型的 Fibonacci 数

Stark 问:什么样的 Fibonacci 数(见 A3)是两个立方数的差或和的一半? 这涉及到求所有类数为 2 的复二次域的问题. 例子: $1=\frac{1}{2}(1^3+1^3), 8=\frac{1}{2}(2^3+2^3), 13=\frac{1}{2}(3^3-1^3)$. Antoniadis 把所有这样的域与某种不定方程的解联系了起来,并对除了两个情形以外的所有情形给出了解答,这两种情形后来由 Weger 所解决.

Cohn 证明了:仅有的 Fibonacci 平方数是 0,1 和 144,Luo Ming 则验证了 Vern Hoggatt 的猜想:Fibonacci 数中仅有的三角数(即形如$\frac{1}{2}m(m+1)$的数)是 0,1,3,21 和 55,后来他又指出:Lucas 数中仅有的三角数是 1,3 和 5778.

参考文献

Jannis A. Antoniadis, Über die Kennzeichnung zweiklassiger imaginär-quadratischer Zahlkörper durch Lösungen diophantisher Gleichungen, *J. reine angew. Math.*, **339**(1983) 27-81; *MR* **85g**:11098.
J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.*, **39**(1964) 537-540; *MR* **29** #1166.
D. G. Gryte, R. A. Kingsley & H. C. Williams, On certain forms of Fibonacci numbers, *Proc. 2nd Louisiana Conf. Combin. Graph Theory & Comput.*, *Congr. Numer.*, **3**(1971) 339–344.
V. E. Hoggatt, Problem 3, *WA St. Univ. Conf. Number Theory*, 1971, p. 225.
Luo Ming, On triangular Fibonacci numbers, *Fibonacci Quart.*, **27**(1989) 98–108; *MR* **90f**:11013.
Luo Ming, On triangular Lucas numbers, *Applications of Fibonacci numbers, Vol.* 4 (1990), 231-240, Kluwer, Dordrecht, 1991; *MR* **93i**:11016.
Neville Robbins, Fibonacci and Lucas numbers of the forms w^2-1, $w^3 \pm 1$, *Fibonacci Quart.*, **19**(1981) 369–373.

H. M. Stark, Problem 23, *Summer Institute on Number Theory*, Stony Brook, 1969.

Ray Steiner, On Fibonacci numbers which are one more than a square, *J. reine angew. Math.*, **262/263**(1973) 171–182.

Ray Steiner, On triangular Fibonacci numbers, *Utilitas Math.*, **9**(1976) 319–327.

M. H. Tallman, Problem H23, *Fibonacci Quart.*, **1**(1963) 47.

Charles R. Wall, On triangular Fibonacci numbers, *Fibonacci Quart.*, **23** (1985) 77–79.

B. M. M. de Weger, A diophantine equation of Antoniadis, *Number Theory and Applications* (Banff, 1988), 547-553, *NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci.*, **265**, Kluwer, 1989; *MR* **92f**:11048.

B. M. M. de Weger, A hyperelliptic Diophantine equation related to imaginary quadratic number fields with class number 2, *J. reine angew. Math.*, **427**(1992) 137–156; *MR* **93d**:11034.

D27. 同 余 数

同余数(congruent number)的取名似乎有点混乱不清,它们与毕达哥拉斯三角形有关,且有悠久的历史. 在一千多年前的一份阿拉伯手稿上就有若干个同余数的例子(5,6,14,表 7 中 CA 条目中的第 17 个数,以及另外 10 个大于 1000 的数). 但是也仅仅是最近 10 年来,由于 Tunnell 的工作,我们才对它们有了比较完全的了解. 它们是使

$$x^2 + ay^2 = z^2 \quad 和 \quad x^2 - ay^2 = t^2$$

同时有整数解的那种整数 a. 它的魅力一部分在于其最小解常常有异乎寻常的大小. 例如 $a = 101$ 是一个同余数,Bastien 给出其最小解:

$$x = 2015242462949760001961,$$
$$y = 118171431852779451900,$$
$$z = 2339148435306225006961,$$
$$t = 1628124370727269996961,$$

而且不管对计算技术和计算机如何改进,可能还需要若干时间才能再发现一些更难征服的同余数. 由 J. A. H. Hunter, M. R. Buckley 和 K. Gallyas 找到的另外一些大的同余数放在本书第一版中.

同余数等价地定义为使不定方程

$$x^4 - a^2y^4 = u^2$$

有解的那种 a.

表 7　小于 1000 的同余数(C)和非同余数(N)

第 c 列和第 r 行的数是 $a = 40c + r$

r \ c	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	NB	C1	□	□	CG	N9	N1	N1	N9	□	N1	□	NJ	N1	CG	N1	N1	N9	C&	C1	□	□	N1	N9	□
2	NB	NB	N2	NX	□	NX	□	NT	NJ	NX	NJ	CG	NT	□	N2	CG	NJ	NJ	□	NJ	NT	NX	□	NX	NL
3	N3	N3	N3	N&	N3	NJ	□	N3	C&	□	NJ	N3	NJ	N3	N3	□	N3	N3	CJ	NJ	NJ	NJ	N3	NJ	□
4	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
5	C5	□	CG	□	CG	CG	□	C&	□	CJ	□	C&	CJ	□	C&	□	C&	CJ	□	□	C&	□	CJ	□	CL
6	C6	C6	C6	□	C6	C6	C&	CA	C6	C&	CJ	C6	□	C6	C6	CJ	CG	□	□	C6	CG	□	C6	C6	CG
7	C7	C7	CG	C7	C7	□	CJ	C&	CJ	C7	CJ	CJ	C7	C&	□	C7	C7	CJ	C7	CJ	CJ	□	C7	□	C7
8	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
9	□	□	N1	N9	□	N9	N9	□	NJ	□	N1	N1	N9	□	N1	C&	N9	C&	□	N1	N1	N9	C&	N1	NJ
10	NX	□	□	NL	N&	CA	□	NL	CA	NL	CG	□	□	NL	NJ	NL	□	NJ	NJ	NJ	□	□	CG	NJ	NJ
11	N3	NB	NB	N3	□	N3	N3	CG	N3	CG	NJ	NJ	N3	□	N3	NJ	CG	N3	C&	NJ	N3	NJ	□	□	N3
12	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
13	C5	C5	CG	CJ	C5	CJ	CJ	C5	□	C5	CJ	CJ	CJ	C&	CL	C5	C5	□	C5	C5	C&	C5	CL	CL	CJ
14	C6	□	C6	C6	CG	C6	C6	□	C6	CJ	□	C6	CJ	CJ	C&	C6	CJ	C6	C6	□	C&	CJ	CJ	C6	C&
15	CA	CG	CG	□	□	C&	CG	CJ	CJ	□	CJ	C&	□	C&	□	C&	CJ	CJ	□	□	CJ	□	CJ	C&	□
16	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
17	N1	N9	N1	C1	N9	NJ	C1	□	N1	NJ	N9	C1	NJ	N9	N1	N1	□	NJ	N9	C&	N9	N1	NT	N1	N1
18	□	NX	□	CG	N2	NX	NJ	NX	□	□	NJ	NX	NJ	NX	□	NJ	C&	NX	□	NX	N2	NJ	NT	NT	NJ
19	N3	N3	□	N3	N3	C&	NJ	CG	NJ	N3	N3	□	N3	□	NJ	N3	N3	NJ	N3	NJ	□	N3	NJ	NT	NJ
20	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
21	CA	C5	C5	C&	C5	CA	□	CJ	CJ	CJ	C5	C5	CJ	C5	CJ	□	C5	C5	CG	CJ	C5	CJ	C&	C5	□
22	C6	C6	CG	C6	C&	CJ	C6	C6	□	C6	C6	CG	C6	C6	C&	C6	C6	□	CJ	CJ	CJ	C6	CJ	CJ	C6
23	C7	□	C7	C&	CJ	C7	C7	CJ	□	C7	□	C7	C7	CL	CG	CL	C&	CJ	C7	□	C7	C7	C&	C&	C7
24	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
25	□	CA	NJ	CG	NJ	□	CG	NJ	NJ	NJ	□	CG	C&	NJ	□	□	NJ	NJ	NJ	NJ	□	NJ	C&	□	C&
26	NX	NB	NX	N2	N&	C&	NJ	□	NX	C&	C&	N2	NJ	CA	NX	N2	□	NT	NX	NJ	NJ	C&	NJ	NJ	NJ
27	□	N3	N3	□	N&	N3	NJ	N3	N3	□	NJ	N3	□	N3	N3	NT	NJ	NJ	□	N3	N3	□	N3	N3	C&
28	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
29	C5	CG	C5	C5	□	C5	C5	CJ	C5	C5	CA	CJ	C5	□	CJ	C&	C&	C5	CJ	CJ	C5	CJ	□	C&	CJ
30	CA	CA	CA	□	CA	CJ	□	CG	□	CA	CJ	CG	CG	□	CJ	□	C&	C&	□	CJ	CJ	C&	C&	□	□
31	C7	C7	CG	C7	C7	CA	C7	C7	□	C&	C7	CJ	C&	CJ	CJ	C7	C&	□	C7	C&	CJ	CJ	C7	C&	C7
32	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
33	N9	N1	N1	□	N1	N1	NJ	C1	C1	N9	N1	N9	□	NJ	N1	N9	N1	NJ	N9	C&	□	□	N9	N1	N9
34	CA	NX	N&	CA	C&	□	N2	NX	NJ	NX	CG	NJ	C&	NX	□	NX	C&	NJ	NL	NX	NJ	NJ	N2	□	NJ
35	NB	□	N&	NJ	NJ	NJ	□	□	NJ	C&	NJ	□	NJ	NJ	NJ	NJ	□	NJ	NJ	NJ	NJ	□	C&	NJ	C&
36	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
37	C5	CG	□	C5	C5	CJ	C5	C5	CG	C5	CJ	□	CG	C5	CL	□	C5	CL	C5	C5	□	C5	CL	C&	C5
38	C6	CG	C6	C6	□	CJ	C6	C&	C6	C6	CG	C6	C&	□	CJ	CJ	CJ	C6	C6	CG	C6	C6	□	C6	C6
39	CG	C7	C&	C&	C7	C7	□	C&	C7	C&	C7	C7	CJ	CJ	C7	□	CJ	C7	CG	C&	C7	C&	C7	C&	□
40	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Dickson 的数论史一书给出许多早期的文献,包括 Fibonacci (Leonardo of Pisa), Genocchi 以及 Gérardin. Gérardin 给出 7,22, 41,69,77,还给出 20 个阿拉伯人的例子和表 7 中标有 CG 的 43 个数. 我们只需要考虑无平方因子的 a 就够了,在小于 1000 的 608 个这样的数中,361 个是同余数,247 个不是同余数. 长期以来人们猜想:无平方因子数是同余数,如果它们模 8 的余数是 5,6 或 7. 现在我们知道此猜想为真(假设关于椭圆曲线的某些得到广

泛认可的猜想为真). 表 7 中标有 C5, C7 以及 C6 的数都是模 8 余 5 或余 7 的素数,或是模 8 余 3 的素数的两倍. Bastien 注意到下面的数都不是同余数:模 8 余 3 的素数,两个这样的素数的乘积,模 8 余 5 的素数的两倍,两个这样的素数的乘积的两倍,以及模 16 余 9 的素数的两倍,这些数在表 7 中分别标以条目 N3, N9, NX, NL 和 N2. 他还给出其他一些非同余数(标有 NB 的数,虽然 $a=1$ 属于 Fermat, 还有其他许多数更早的时候已为比如说 Genocchi 所知晓),他说道:a 不是一个同余数,如果它是模 8 同余于 1 的素数,且 $a=b^2+c^2$, $b+c$ 是 a 的非剩余(见 F5),这对于条目标号为 N1 的一些数给出了解释.

注意,表中条目上标有 1,3,5,7 的数用来作为模 8 的相应的剩余类中的素数表.

条目 C& 和 N& 取自 Alter, Curtz 和 Kubota, 而 CJ 和 NJ 则取自 Jean Lagrange 的学位论文.

参考文献

Ronald Alter, The congruent number problem, *Amer. Math. Monthly*, **87** (1980) 43–45.

R. Alter & T. B. Curtz, A note on congruent numbers, *Math. Comput.*, **28**(1974) 303–305; *MR* **49** #2527 (not #2504 as in *MR* indexes); correction **30**(1976) 198; *MR* **52** #13629.

R. Alter, T. B. Curtz & K. K. Kubota, Remarks and results on congruent numbers, *Proc. 3rd S.E. Conf. Combin. Graph Theory Comput., Congr. Numer.* **6** (1972) 27–35; *MR* **50** #2047.

L. Bastien, Nombres congruents, *Intermédiaire Math.*, **22**(1915) 231–232.

B. J. Birch, Diophantine analysis and modular functions, *Proc. Bombay Colloq. Alg. Geom.*, 1968.

J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.*, **41**(1966) 193–291.

L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Diophantine Analysis, Washington, 1920, 459–472.

A. Genocchi, Note analitiche sopra Tre Sritti, *Annali di Sci. Mat. e Fis.*, **6**(1855) 273–317.

A. Gérardin, Nombres congruents, *Intermédiaire Math.*, **22**(1915) 52–53.

H. J. Godwin, A note on congruent numbers, *Math. Comput.*, **32** (1978) 293–295; **33** (1979) 847; *MR* **58** #495; **80c**:10018.

Jean Lagrange, Thèse d'Etat de l'Université de Reims, 1976.

Jean Lagrange, Construction d'une table de nombres congruents, *Bull. Soc. Math. France Mém.* No. 49–50 (1977) 125–130; *MR* **58** #5498.

Paul Monsky, Mock Heegner points and congruent numbers, *Math. Z.*, **204** (1990) 45–68; *MR* **91e**:11059.

Paul Monsky, Three constructions of rational points on $Y^2 = X^3 \pm NX$, *Math. Z.*, **209**(1992) 445–462; *MR* **93d**:11058.

L. J. Mordell, *Diophantine Equations*, Academic Press, London, 1969, 71–72.

Kazunari Noda & Hideo Wada, All congruent numbers less than 10000, *Proc. Japan Acad. Ser. A Math. Sci.*, **69**(1993) 175–178.

S. Roberts, Note on a problem of Fibonacci's, *Proc. London Math. Soc.*, **11**(1879–80) 35–44.

P. Serf, Congruent numbers and elliptic curves, in *Computational Number Theory* (Proc. Conf. Number Theory, Debrecen, 1989), de Gruyter, 1991, 227–238; *MR* **93g**:11068.

N. M. Stephens, Congruence properties of congruent numbers, *Bull. London Math. Soc.*, **7**(1975) 182–184; *MR* **52** #260.

Jerrold B. Tunnell, A classical diophantine problem and modular forms of weight 3/2, *Invent. Math.* **72**(1983) 323–334; *MR* **85d**:11046.

D28. 一个倒数不定方程

Mordell 要求

$$\frac{1}{w}+\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{wxyz}=0$$

的整数解. 迄今已有若干论文发表,这些论文给出了参数解族. 例如,Takahiro Nagashima 给出了 Mordell 方程的解:

$$(w,x,y,z)=(5,3,2,-1),(-7,-3,-2,1),(31,-5,-3,2),$$
$$(1366,-15,7,-13),(n+1,-n-1,1),$$

更一般地有 $w=xyz+1$,其中

$$x=-2\varepsilon h^3-\delta\varepsilon h^2(n-3)+\varepsilon h(n-1-2\delta\varepsilon)+1$$
$$y=2\delta\varepsilon h^2+\varepsilon h(n-3)-\varepsilon\delta(n-1)+1,$$
$$z=-2\delta\varepsilon h^2-\varepsilon h(n-1)-1,$$

这里相互独立地有 $\varepsilon,\delta=\pm1$,但是似乎并不能保证这 4 个双参数族一定给出所有的解.

张明志(Zhang Ming-Zhi)指出怎样得到给定界限以内的所有的解,而 Clellie Oursler 和 Judith Longyear 给出深入的分析,他们每人都给出一个求所有解的程序. 代替 Mordell 的 $n = 4$, Longyear 的程序延拓到了 $n(\geqslant 3)$个变量的 x_i 的方程 $\sum(1/x_i) + \prod(1/x_i) = 0$.

参考文献

Lawrence Brenton & Daniel S. Drucker, On the number of solutions of $\sum_{j=1}^{s}(1/x_j) + 1/(x_1 \cdots x_s) = 1$, *J. Number Theory*, **44**(1993) 25–29.

Cao Zhen-Fu, Mordell's problem on unit fractions. (Chinese. English summary) J. Math. (Wuhan) **7**(1987) 239–244; *MR* **90a**:11032.

Sadao Saito, A diophantine equation proposed by Mordell (Japanese. English summary), *Res. Rep. Miyagi Nat. College Tech. No.* 25 (1988) 101–106; II, *No.* 26 (1990) 159–160; *MR* **91c**:11016–7.

Chan Wah-Keung, Solutions of a Mordell Diophantine equation, *J. Ramanujan Math. Soc.*, **6**(1991) 129-140; *MR* **93d**:11033.

Wen Zhang-Zeng, Investigation of the integer solutions of the Diophantine equation $1/w+1/x+1/y+1/z+1/wxyz = 0$ (Chinese) *J. Chengdu Univ. Natur. Sci.*, **5**(1986) 89–91; *MR* **89c**:11051.

Zhang Ming-Zhi, On the diophantine equation $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w} + \frac{1}{xyzw} = 0$, *Acta Math. Sinica (N.S.)*, **1**(1985) 221–224; *MR* **88a**:11033.

E. 整数序列

这里我们主要(但并非全部)关心无穷序列,这和 C、A 两章的内容会有所重复. 有关这个论题的一部极好的教材和问题来源是 H. Halberstam 和 K. F. Roth 的书 *Sequences*(第二版,Springer-Verlag, New York, 1982),其他的文献是:

P. Erdős, A. Sárközi & E. Szemerédi, On divisibility properties of sequences of integers, in *Number Theory, Colloq. Math. Soc. János Bolyai*, **2**, North-Holland, 1970, 35–49.

H. Ostmann, *Additive Zahlentheorie* I, II, Springer-Verlag, Heidelberg, 1956.

Carl Pomerance & András Sárközi, Combinatorial Number Theory, in R. Graham, M. Grötschel & L. Lovász (editors) *Handbook of Combinatorics*, North-Holland, Amsterdam, 1994.

A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I, II, *J. reine angew. Math.*, **194**(1955) 40–65, 111–140; *MR* **17**, 713.

Paul Turán (editor), *Number Theory and Analysis; a collection of papers in honor of Edmund Landau* (1877–1938), Plenum Press, New York, 1969, contains several papers, by Erdős and others, on sequences of integers.

我们将用 $\mathscr{A}=\{a_i\}, i=1,2,\cdots$ 来表示一个可能是无穷的、严格增加的非负整数序列. 不超过 x 的元素 a_i 的个数记为 $A(x)$. 所谓一个序列的密度指的是 $\lim A(x)/x$,如果它存在的话.

E1. 所有数都等于某个元素加上一个素数的薄序列

Erdös 悬赏 50 美元给解决下述问题者:是否存在一个足够薄的序列,使 $A(x)<c\ln x$,但是每个充分大的整数都可以表成形式 $p+a_i$,其中 p 是一个素数?

对于用平方数代替素数得到的类似的问题,Leo Moser 证明了对某个 $c>0$ 有 $A(x)>(1+c)\sqrt{x}$,而 Erdös 证明了存在一个序列使 $A(x)<c\sqrt{x}$. Moser 对 c 给出的最好的值是 0.06,这被

Abbott改进为 0.147，被 Balasubramanian 和 Soundarajan 改进为 0.245，被 Cilleruelo 改进为 0.273. 对 r 次幂，Cilleruelo 得到

$$A(x) > \frac{x^{1-\frac{1}{r}}}{\Gamma\left(2-\frac{1}{r}\right)\Gamma\left(1+\frac{1}{r}\right)}.$$

对于用 2 的幂来代替素数所得到的问题，Ruzsa 得到了与 Erdös 类似的结果，但是并不知道是否存在常数 $c>0$，使得每个正整数都可以表为形式 $a_i+2^k(a_i\in\mathscr{A})$ 的序列 $\mathscr{A}$ 都满足 $A(x)>(1+c)\log_2 x$？

参考文献

H. L. Abbott, On the additive completion of sets of integers, *J. Number Theory*, **17**(1983) 135–143.

R. Balasubramanian & K. Soundarajan, On the additive completion of squares, II, *J. Number Theory*,**40**(1992) 127–129.

Javier Cilleruelo, The additive completion of kth powers, *J. Number Theory*, **44**(1993) 237–243.

P. Erdős, Problems and results in additive number theory, *Colloque sur la Théorie des Nombres, Bruxelles*, 1955, 127–137, Masson, Paris, 1956.

L. Moser, On the additive completion of sets of integers, *Proc. Symp. Pure Math.*, **8**(1965) Amer. Math. Soc., Providence RI, 175–180.

I. Ruzsa, On a problem of P. Erdős, *Canad. Math. Bull.*, **15**(1972) 309–310.

E2. 每对数的最小公倍数都小于 x 的序列之密度

如果序列的每一对元素的最小公倍数$[a_i,a_j]$至多为 x，那么 $A(x)$的最大值是什么？已知有

$$(9x/8)^{1/2}\leqslant \max A(x)\leqslant(4x)^{1/2}.$$

其下界可以这样得到：将所有的数从 1 取到$\sqrt{x/2}$，而将偶数取到$\sqrt{2x}$.

对给定的 t，我们能找到多少个小于 x 的数，使得其中任何一对数的最大公因子都小于 t 呢？如果 $t<n^{\frac{1}{2}+\epsilon}$，则这种数的个数 $\sim\pi(n)$；而如果 $t=n^{\frac{1}{2}+c}$，则该数$\sim(1+c')\pi(n)$.

Erdös 还要求 $B(x)$的界,这里 $B(x)$定义为满足如下性质的最小的数:$[1,x]$的任何基数为 $B(x)$的子集都包含三个数,它们两两有同样的最小公倍数. 可能有$B(x)=o(x)$. 再次令 $C(x)$表示相应的最小的基数,于是总有 3 个数存在,它们两两有同样的最大公因子. 毫无疑问有

$$¿\quad e^{c_1(\ln x)^{1/2}} < C(x) < e^{c_2(\ln x)^{1/2}} \quad ?$$

但是 Erdös 证明的最好的结果是 $C(x)<x^{3/4}$.

给定一个序列 $A, a_1<a_2<\cdots$, Erdös 和 Szemerédi 用 $F(A,x,k)$来记使得最小公倍数$[a_{i+1},a_{i+2},\cdots,a_{i+k}]<x$ 成立的 i 的个数,并问下述结论是否为真:对每个 $\varepsilon>0$都存在一个 k,使$F(A,x,k)<x^{\varepsilon}$? 他们证明了:对每个 A 有 $F(A,x,3)<c_1x^{1/3}\ln x$,且存在一个 A,对无穷多个 x 有 $F(A,x,3)>c_2x^{1/3}\ln x$,但他们并不知道是否有一个 A 使此式对所有 x 为真.

Graham, Spencer 和 Witsenhausen 问:永远不出现$\{n,2n,3n\}$的整数序列的密度能有多大?

在 Erdös, Sárközy 和 Szemerédi 的论文中有此领域中详尽的文献目录和许多未解决的问题. 也见问题 B24 的参考文献.

参 考 文 献

P. Erdős, Problem, *Mat. Lapok* **2**(1951) 233.

P. Erdős & A. Sárközy, On the divisibility properties of sequences of integers, *Proc. London Math. Soc.* (3), **21**(1970) 97–100; *MR* **42** #222.

P. Erdős, A. Sárközy & E. Szemerédi, On divisibility properties of sequences of integers, in Number Theory *Colloq. Janós Bolyai Math. Soc., Debrecen 1968*, North-Holland, Amsterdam (1970) 35–49; *MR* **43** #4790.

P. Erdős & E. Szemerédi, Remarks on a problem of the *American Mathematical Monthly, Mat. Lapok*, **28**(1980) 121–124; *MR* **82c**:10066.

R. L. Graham, J. H. Spencer & H. S. Witsenhausen, On extremal density theorems for linear forms, in H. Zassenhaus (ed), *Number Theory and Algebra*, Academic Press, New York, 1977, 103–109; *MR* **58** #569.

E3. 有两个大小可比的因子的整数序列之密度

"整数

$$6,\ 12,\ 15,\ 18,\ 20,\ 24,\ 28,\ 30,\ 35,\ 36,\ 40,$$
$$42,\ 45,\ 48,\ 54,\ 56,\ 60,\ 63,\ 66,\ 70,\ 72,\ \cdots$$

(它们有两个因子 d_1, d_2 适合 $d_1<d_2<2d_1$)的密度为 1"这一结论是否为真? Erdös 证明了它的密度存在. 它和覆盖同余系(F13)有联系. 自从本书第一版问世以来,这个问题已经由 Maier 和 Tenenbaum 给出了肯定的回答.

参 考 文 献

P. Erdős, On the density of some sequences of integers, *Bull. Amer. Math. Soc.*, **54**(1948) 685–692; *MR* **10**, 105.

Helmut Maier & G. Tenenbaum, On the set of divisors of an integer, *Invent. Math.*, **76**(1984) 121–128; *MR* **86b**:11057.

E4. 无一能整除其他 r 个数之积的序列

如果序列 $\{a_i\}$ 中没有元素能整除 r 个其他的项的乘积,则 Erdös 证明了

$$\pi(x)+c_1x^{2/(r+1)}(\ln x)^{-2}<A(x)<\pi(x)+c_2x^{2/(r+1)}(\ln x)^{-2},$$

这里 $\pi(x)$是$\leqslant x$ 的素数个数. 然而,如果我们假设任何个数不多于 r 的那么多个 a_i 的乘积都是不同的,那么 $\max A(x)$会有多大呢? 对 $r\geqslant 3$,Erdös 证明了

$$\max A(x)<\pi(x)+O(x^{2/3+\varepsilon}).$$

如果 $r=1$,则没有哪一项能整除另外任何一项,该序列称为本原的(primitive). 张振祥(Zhang Zhen-Xiang)证明了:对于那种每个元素至多有 4 个素因子的本原序列,当 $n>1$ 时有

$$\sum_{a_i\leqslant n}\frac{1}{a_i\ln a_i}\leqslant\sum_{p\leqslant n}\frac{1}{p\ln p}$$

(从而小于 1.64),这里的和分别取过序列中直到 n 的所有元素以及直到 n 的所有素数.

参考文献

P. Erdős, On sequences of integers no one of which divides the product of two others and on some related problems, *Inst. Math. Mec. Tomsk*, **2**(1938) 74–82.

P. Erdős, Extremal problems in number theory V (Hungarian), *Mat. Lapok*, **17**(1966) 135–155.

P. Erdős, On some applications of graph theory to number theory, *Publ. Ramanujan Inst.*, **1**(1969) 131–136.

P. Erdős & Zhang Zhen-Xiang, Upper bound of $\sum 1/(a_i \log a_i)$ for primitive sequences, *Proc. Amer. Math. Soc.*, **117**(1993) 891–895.

Zhang Zhen-Xiang, On a conjecture of Erdős on the sum $\sum_{p\le n} 1/(p\log p)$, *J. Number Theory*, **39**(1991) 14–17; *MR* **92f**:11131.

Zhang Zhen-Xiang, On a problem of Erdős concerning primitive sequences, *Math. Comput.*, **60**(1993) 827–834; *MR* **93k**:11120.

E5. 可被给定集中至少一个数整除的数组成之序列

设 $D(x)$ 是不大于 x 且可被至少一个 a_i 整除的那种数的个数，这里 $a_1<a_2<\cdots<a_k\leqslant n$ 是一个有限序列. 对所有 $x>n$ 有 $D(x)/x<2D(n)/n$ 吗? 这里的数 2 不能减小：例如 $n=2a_1-1, x=2a_1<a_2$. 在其他方向上已知有：对每个 $\varepsilon>0$，存在一个不满足不等式 $D(x)/x>\varepsilon D(n)/n$ 的序列.

参考文献

A. S. Besicovitch, On the density of certain sequences, *Math. Ann.*, **110**(1934) 335–341.

P. Erdős, Note on sequences of integers no one of which is divisible by any other, *J. London Math. Soc.*, **10**(1935) 126–128.

E6. 每对数之和均不在给定序列中的数组成之序列

设 $n_1<n_2<\cdots$ 是一个整数序列，$n_{i+1}/n_i\to 1$（$i\to\infty$ 时），且对每个 d，$\{n_i\}$ 模 d 一致分布，即对每个 $c(0\leqslant c<d)$ 和所有 d，满足 $n_i\leqslant x(n_i\equiv c \bmod d)$ 的数 n_i 的个数 $N(c,d;x)$ 适合

$$N(c,d;x)/N(1,1;x)\to 1/d\quad(\text{当 } x\to\infty \text{ 时}).$$

如果 $a_1<a_2<\cdots$是一个无穷序列,对任何 i,j,k,有 $a_j+a_k\neq n_i$,则 Erdös 问:a_j 的密度小于$\frac{1}{2}$是否为真?

E7. 与素数有关的级数和序列

如果 p_n 是第 n 个素数,Erdös 问 $\sum(-1)^n n/p_n$ 是否收敛?他注意到级数 $\sum(-1)^n(n\ln n)/p_n$ 发散.

他又问:给定 3 个不同的素数,而 $a_1<a_2<a_3<\cdots$都是这 3 个素数的幂的乘积(按照增加的次序排列),是否有无穷多对 a_i 和 a_{i+1},使它们都是素数幂呢? 又如果我们用 k 个素数甚至无穷多个素数来代替 3 个素数,会得到什么结论? Meyer 和 Tijdeman 对两个有限素数集 S 和 T 以及由 $S\cup T$ 所形成的序列 $a_1<a_2<a_3<\cdots$问了一个类似的问题. 是否存在无穷多个 i,使得 a_i 是 S 中素数的幂的乘积,而 a_{i+1}则是 T 中素数的幂的乘积呢?

E8. 任一对数之和均非平方数的序列

Paul Erdös 和 David Silverman 考虑了 k 个整数 $1\leqslant a_1<a_2<\cdots<a_k\leqslant n$,其中任意两个数的和 a_i+a_j 都不是平方数. $k<n(1+\varepsilon)/3$ 是否为真? 甚至会有 $k<n/3+O(1)$吗? 模 3 余 1 的整数表明,如果这一结论为真,那么它是最好可能的. 他们建议在用其他的序列取代平方数后再提出同样的问题.

Erdös 和 Graham 在证明过程中在他们的书中又写道:J. P. Marsias 发现了,任何两个模 32 同余于 1,5,9,13,14,17,21,25,26,29,30 的整数之和模 32 绝不是一个平方数,因此 k 最小可以取到 $11n/32$. 对于该问题的模的形式,这是最好可能的结果了,因为 Lagarias, Odlyzko 和 Shearer 已经证明了:如果 $S\subseteq Z_n$ 且 $S+S$不包含Z_n 的平方数,那么有$|S|\leqslant 11n/32$.

参考文献

J. C. Lagarias, A. M. Odlyzko & J. B. Shearer, On the density of sequences of integers the sum of no two of which is a square, I. Arithmetic progressions, *J. Combin. Theory Ser. A*, **33**(1982) 167–185; II. General sequences, **34**(1983) 123–139; *MR* **85d**:11015ab.

E9. 把整数分划成有大量数对和的类

K. F. Roth 猜想存在绝对常数 c，使对每个 k，存在一个 $n_0 = n_0(k)$ 具有下述性质：对 $n > n_0$，把不超过 n 的整数分划成 k 个类 $\{a_i^{(j)}\}(1 \leqslant j \leqslant k)$，那么不超过 n 且对某个 j 能表为形式 $a_{i_1}^{j} + a_{i_2}^{(j)}$ 的不同整数的个数大于 cn. 此猜想已被 Erdös, Sárközy 和 Sós 证明.

他们还对用乘积代替和产生的相应的问题进行了研究，但其中 $k=2$ 的问题仍未获得解决.

参考文献

P. Erdős & A. Sárközy, On a conjecture of Roth and some related problems, II, in R. A. Mollin (ed.) *Number Theory*, Proc. 1st Conf. Canad. Number Theory Assoc., Banff 1988, de Gruyter, 1990, 125–138.

P. Erdős, A. Sárközy & V. T. Sós, On a conjecture of Roth and some related problems, I, *Colloq. Math. Soc. János Bolyai* (1992).

E10. van der Waerden 定理；Szemerédi 定理；整数分类使至少一个类包含一个算术级数

熟知的 van der Waerden 定理说的是：对每个 l，存在一个数 $n(h, l)$，使得如果不超过 $n(h, l)$ 的整数被分划成 h 个类，那么其中至少有一个类包含一个有 $l+1$ 个项的算术级数. 更一般地，给定 $l_0, l_1, \cdots, l_{h-1}$，总存在一个类 $V_i(0 \leqslant i \leqslant h-1)$，它包含一个有 l_i+1 项的算术级数. 用 $W(h, l)$（或者更一般地用 $W(h; l_0,$

$l_1,\cdots,l_{h-1}$))来表示最小的这样的 $n(h,l)$.

Chvátal 计算出 $W(2;2,2)=9$, $W(2;2,3)=18$, $W(2;2,4)=22$, $W(2;2,5)=32$ 以及 $W(2;2,6)=46$;Beeler 和 O'Neil 给出 $W(2;2,7)=58$, $W(2;2,8)=77$ 以及 $W(2;2,9)=97$. Chvátal 发现了 $W(2;3,3)=35$ 和 $W(2;3,4)=55$;Beeler 和 O'Neil 发现了 $W(2;3,5)=73$. Stevens 和 Shantaram 找到了 $W(2;4,4)=178$; Chvátal 找到了 $W(3;2,2,2)=27$;而 Brown 找到了 $W(3;2,2,3)=51$. Beeler 和 O'Neil 又发现了 $W(4;2,2,2,2)=76$.

van der Waerden 定理的许多证明都只给出 $W(h,l)$的不太好的估计. Erdös 和 Rado 证明了 $W(h,l)>(2lh^l)^{\frac{1}{2}}$,而 Moser, Schmidt 和 Berlekamp 相继将它改进为

$$W(h,l) > lh^{c\ln n} \quad 和 \quad W(h,l) > h^{l+1-c\sqrt{(l+1)(\ln(l+1))}}.$$

对 $l \geqslant 5$, Moser 的界被 Abbott 和 Liu 改进为

$$W(h,l) > h^{c_s(\ln h)^s},$$

这里 s 由 $2^s \leqslant l < 2^{s+1}$ 来定义,而 Everts 证明了 $W(h,l) > lh^l/4(l+1)^2$,这个结果有时比 Berlekamp 的结果要好. 对 $h=2$, Szabó 最近证明了 $W(2,l)>2^l/l^\varepsilon$. 所有的上界都是"ackermanic"般大小,直到 Shelah 的证明把它们变成了"wowser"——有关这些词语的解释见 Graham, Rothschild 和 Spencer 的书.

多年以前由 Erdös 和 Turán 引入了一个与此密切相关的函数(对 $l+1=k$),即现在广为人知的 $r_k(n)$:它定义为使得有 r 个不超过 n 的数的序列 $1 \leqslant a_1 < a_2 < \cdots < a_r \leqslant n$ 必定包含一个有 k 个项的算术级数的最小的 r. 当 $k=3$ 时最好的界属于 Behrend, Roth 和 Moser:

$$n\exp\left(-c_1\sqrt{\ln n}\right) < r_3(n) < c_2 n/\ln \ln n.$$

对更大的 k, Rankin 证明了

$$r_k(n) > n^{1-c_s/(\ln n)^{s/(s+1)}},$$

其中 s 与前一样由 $2^s < k \leqslant 2^{s+1}$ 来定义.

一个重要的突破是 Szemerédi 证明了对所有 k 有 $r_k(n)=o(n)$，然而，不论是他的证明，还是 Furstenberg 以及 Katznelson 和 Ornstein 的证明(见 Thouvenot 的著作)都没有给出 $r_k(n)$的估计. Erdös 猜想有

$$¿\quad r_k(n) = o(n(\ln n)^{-t}) \quad (\text{对每个 } t) \quad ?$$

这一猜想蕴含:对每个 k，有 k 个素数在算术级数中. 有关 Erdös 的一个有可能赢得报酬的猜想请见 A5，如果该猜想为真，就可以推出 Szemerédi 定理.

另一个与之密切相关的问题由 Leo Moser 考虑过，他把整数用以 3 为底的形式写出，即，$n=\sum a_i3^i$ ($a_i=0,1$ 或 2)并检查了 n 映射成无穷维 Euclid 空间中的格点$(a_1,a_2,a_3,\cdots)$的映射. 他称若干个整数是共线的(collinear)，如果它们的象共线. 例如，35 $\to(2,2,0,1,0,\cdots)$，41$\to(2,1,1,1,0,\cdots)$和 47$\to(2,0,2,1,0,\cdots)$是共线的. 他猜想:每个无三项共线的整数序列的密度皆为零. 如果整数共线，它们就在算术级数中，但反之未必成立(例如:16$\to(1,2,1,0,0,\cdots)$，24$\to(0,2,2,0,0,\cdots)$和32$\to(2,1,0,1,0,\cdots)$不共线). 因此，这一猜想为真就蕴含 Roth 定理 $r_3(n)=o(n)$.

如果 $f_3(n)$是每一边上有三点的 n 维立方体中无三点共线的格点的最大个数，则 Moser 证明了 $f_3(n)>c3^n/\sqrt{n}$. 易见 $f_3(n)/3^n$ 有极限，它的极限是零吗? Chvátal 把 Moser 的结果中的常数改进为 $3/\sqrt{\pi}$，并求得 $f_3(1)=2, f_3(2)=6, f_3(3)=16$. 又已知有 $f_3(4)\geqslant 43$.

更一般地，如果 n 维立方体每一边上有 k 个点，Moser 要求无 k 点共线的格点的最大个数 $f_k(n)$的估计. 下述结论是 Hales 和 Jewett 的一个定理对 n 维画连城游戏(tic-tac-toe)的应用:对充分大的 n，k^n 个格点分成 h 个类的任一种分化都含有一个类，其中必有 k 点共线. 这蕴含 van der Waerden 定理，只要让点$(a_1,a_2,\cdots,a_{n-1})$(这里 $0\leqslant a_i\leqslant k-1$)与整数展开成 $\sum a_ik^i$ 的基数 k 相对应即可. 还不知道对每个 c 和充分大的 n，是否可能取到

$ck^n/\sqrt{n}$个点，其中没有 k 个点共线？对某种 c 结论是已知的．下面引用的 Riddell 的第二篇论文中的不等式(4)蕴含

$$f_k(n) > k^{n+1}/(2\pi e^3(k-1)n)^{\frac{1}{2}},$$

因此对某个 c 我们可以选取 $ck^n/\sqrt{n}$ 个点的"无线集"("line-free" set)．在其他的方向上，他得到 $f_3(n) \leqslant 16 \cdot 3^{n-3}$．他感谢 Leo Moser 在他得到这些结果时所给予的鼓励．

如果你用贪婪算法(greedy algorithm)来构造不包含算术级数的序列，你将得不到很稠密的序列，但是你的确可以得到某些有意思的序列．Odlyzko 和 Stanley 构造出了正整数序列 $S(m)$，其中 $a_0=0, a_1=m$，而每一个后面的项 a_{n+1} 是大于 a_n 且使得 $a_0, a_1, \cdots, a_{n+1}$ 不包含一个有三项的算术级数的最小的数．例如

$S(1)$：0,1,3,4,9,10,12,13,27,28,30,31,36,37,39,40,81,82,84,95,90,91,93,94,108,109,111,112,117,118,120,…

$S(4)$：0,4,5,7,11,12,16,23,26,31,33,37,38,44,49,56,73,78,80,85,95,99,106,124,128,131,136,143,…

如果 m 是 3 的幂，或是 3 的幂的两倍，那么该序列的元素刻画起来较为容易(将 $S(1)$ 用 3 为基数写出)，但对其他的值，该序列的性状则无明显的规律．它们增长的速率似乎类似，但这并没有得到证明．

不包含四项算术级数的这种"最简单的"序列是

0,1,2,4,5,7,8,9,14,15,16,18,25,26,28,29,30,33,36,
48,49,50,52,53,55,56,57,62,…

对于它是否有简单的表述呢？它增长得有多快？

如果我们定义集合 S 的间距(span)为 $\max S - \min S$，那么一个不包含有 k 个项的算术级数的、有 n 个整数的集合的最小间距 $sp(k,n)$ 等于什么？Zalman Usiskin 给出下面的值

$n=$	3	4	5	6	7	8	9	10	11…
$sp(3,n)=$	3	4	8	10	12	13	19	24	25…
$sp(4,n)=$	4	5	7	8	9	12…			

Abbott 注意到由 Szemerédi 定理推出：对每个 $k\geqslant 3$，序列 $\{sp(k,n+1)-sp(k,n)\}$ 是无界的，并且问：它是否包含一个有界的子序列？

Alfred Brauer 的一篇论文以及与 E10~E14 这几节有关的、有意义的早期文献，请参考 F6 中所述.

参 考 文 献

H. L. Abbott & D. Hanson, Lower bounds of certain types of van der Waerden numbers, *J. Combin. Theory*, **12**(1972) 143–146.

H. L. Abbott & A. C. Liu, On partitioning integers into progression free sets, *J. Combin. Theory*, **13**(1972) 432–436.

H. L. Abbott, A. C. Liu & J. Riddell, On sets of integers not containing arithmetic progressions of prescribed length, *J. Austral. Math. Soc.*, **18**(1974) 188–193.

Michael D. Beeler & Patrick E. O'Neil, Some new van der Waerden numbers, *Discrete Math.*, **28**(1979) 135–146.

F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. USA* **32**(1946) 331-332; *MR* **8**, 317.

E. R. Berlekamp, A construction for partitions which avoid long arithmetic progressions, *Canad. Math. Bull.*, 11(1968) 409–414.

E. R. Berlekamp, On sets of ternary vectors whose only linear dependencies involve an odd number of vectors, *Canad. Math. Bull.*, **13**(1970) 363–366.

Thomas C. Brown, Some new Van der Waerden numbers, Abstract 74T-A113, *Notices Amer. Math. Soc.*, **21**(1974) A-432.

T. C. Brown, Behrend's theorem for sequences containing no k-element progression of a certain type, *J. Combin. Theory Ser. A*, **18**(1975) 352–356.

Ashok K. Chandra, On the solution of Moser's problem in four dimensions, *Canad. Math. Bull.*, **16**(1973) 507–511.

V. Chvátal, Some unknown van der Waerden numbers, in *Combinatorial Structures and their Applications*, Gordon and Breach, New York, 1970, 31–33.

J. A. Davis, Roger C. Entringer, Ronald L. Graham & G. J. Simmons, On permutations containing no long arithmetic progressions, *Acta Arith.*, **34**(1977/78) 81-90; *MR* **58** #10705.

P. Erdős, Some recent advances and current problems in number theory, in *Lectures on Modern Mathematics*, Wiley, New York, **3**(1965) 196–244.

P. Erdős & R. Rado, Combinatorial theorems on classifications of subsets of a given set, *Proc. London Math. Soc.*(3), **2**(1952) 417–439; *MR* **16**, 445.

P. Erdős & J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press, 1974, 37-39.

P. Erdős & P. Turán, On some sequences of integers, *J. London Math. Soc.*, **11**(1936) 261-264.

F. Everts, PhD thesis, Univ. of Colorado, 1977.

H. Furstenberg, Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. Analyse Math.*, **31**(1977) 204–256; *MR* **58** #16583.

Joseph L. Gerver & L. Thomas Ramsey, Sets of integers with no long arithmetic progressions generated by the greedy algorithm, *Math. Comput.*, **33**(1979) 1353–1359; *MR* **80k**:10053.

Joseph Gerver, James Propp & Jamie Simpson, Greedily partitioning the natural numbers into sets free of arithmetic progressions, *Proc. Amer. Math. Soc.*, **102**(1988) 765–772

R. L. Graham & B. L. Rothschild, A survey of finite Ramsey theorems, *Proc. 2nd Louisiana Conf. Combin., Graph Theory, Comput., Congr. Numer.*, **3**(1971) 21–40.

R. L. Graham & B. L. Rothschild, A short proof of van der Waerden's theorem on arithmetic progressions, *Proc. Amer. Math. Soc.*, **42**(1974) 385–386.

Ronald L. Graham, Bruce L. Rothschild & Joel H. Spencer, *Ramsey Theory*, 2nd edition, Wiley-Interscience, 1990.

G. Hajós, Über einfache und mehrfache Bedeckungen des n-dimensionalen Raumes mit einem Würfelgitter. *Math. Z.*, **47**(1942) 427–467.

A. W. Hales & R. I. Jewett, Regularity and positional games, *Trans. Amer. Math. Soc.*, **106**(1963) 222–229.

A. Y. Khinchin, *Three Pearls of Number Theory*, Graylock Press, Rochester NY, 1952, 11-17.

Bruce M. Landman & Raymond N. Greenwell, Some new bounds and values for van der Waerden-like numbers, *Graphs Combin.*, **6**(1990) 287–291; *MR* **91k**:11023.

L. Moser, On non-averaging sets of integers, *Canad. J. Math.*, **5**(1953) 245-252; *MR* **14**, 726d, 1278.

Leo Moser, Notes on number theory II. On a theorem of van der Waerden, *Canad. Math. Bull.*, **3**(1960) 23–25; *MR* **22** #5619.

L. Moser, Problem 21, *Proc. Number Theory Conf.*, Univ. of Colorado, Boulder, 1963, 79.

L. Moser, Problem 170, *Canad. Math. Bull.*, **13**(1970) 268.

A. M. Odlyzko & R. P. Stanley, Some curious sequences constructed with the greedy algorithm, Bell Labs. internal memo, 1978.

Carl Pomerance, Collinear subsets of lattice-point sequences – an analog of Szemerédi's theorem, *J. Combin. Theory Ser. A*, **28**(1980) 140–149; *MR* **81m**: 10104.

Jim Propp, What are the laws of greed?, *Amer. Math. Monthly*, **96**(1989) 334–336.

John R. Rabung, On applications of van der Waerden's theorem, *Math. Mag.*, **48**(1975) 142–148.

John R. Rabung, Some progression-free partitions constructed using Folkman's method, *Canad. Math. Bull.*, **22**(1979) 87–91.

R. Rado, Note on combinatorial analysis, *Proc. London Math. Soc.*, **48**(1945) 122–160.

R. A. Rankin, Sets of integers containing not more than a given number of terms

in arithmetical progression, *Proc. Roy. Soc. Edinburgh Sect. A*, **65** (1960/61) 332–334; *MR* **26** #95.

J. Riddell, On sets of numbers containing no l terms in arithmetic progression, *Nieuw Arch. Wisk.* (3), **17**(1969) 204–209; *MR* **41** #1678.

J. Riddell, A lattice point problem related to sets containing no l-term arithmetic progression, *Canad. Math. Bull.*, **14**(1971) 535–538; *MR* **48** #265.

K. F. Roth, Sur quelques ensembles d'entiers, *C.R. Acad. Sci. Paris*, **234** (1952) 388–390.

K. F. Roth, On certain sets of integers, *J. London Math. Soc.*, **28**(1953) 104–109 (& see **29**(1954) 20–26); *MR* **14**, 536; *J. Number Theory*, **2**(1970) 125–142; *Period. Math. Hungar.*, **2**(1972) 301–326.

R. Salem & D. C. Spencer, On sets of integers which contain no three terms in arithmetical progession, *Proc. Nat. Acad. Sci.*, **28**(1942) 561–563; *MR* **4**, 131.

R. Salem & D. C. Spencer, On sets which do not contain a given number in arithmetical progession, *Nieuw Arch. Wisk.* (2), **23**(1950) 133–143.

H. Salié, Zur Verteilung natürlicher Zahlen auf elementfremde Klassen, *Ber. Verh. Sächs. Akad. Wiss. Leipzig*, **4**(1954) 2–26.

Wolfgang M. Schmidt, Two combinatorial theorems on arithmetic progressions, *Duke Math. J.*, **29**(1962) 129–140.

S. Shelah, Primitive recursive bounds for van der Waerden numbers, *J. Amer. Math. Soc.*, **1**(1988) 683–697; *MR* **89a**:05017.

G. J. Simmons & H. L. Abbott, How many 3-term arithmetic progressions can there be if there are no longer ones? *Amer. Math. Monthly*, **84**(1977) 633–635; *MR* **57** #3056.

R. S. Stevens & R. Shantaram, Computer generated van der Waerden partitions, *Math. Comput.*, **32**(1978) 635–636.

Zoltán István Szabó, An application of Lovász' local lemma—a new lower bound for the van der Waerden number, *Random Structures Algorithms*, **1**(1990) 343–360; *MR* **92c**:11011.

E. Szemerédi, On sets of integers containing no four terms in arithmetic progression, *Acta Math. Acad. Sci. Hungar.*, **20**(1969) 89–104.

E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.*, **27**(1975) 199–245.

J. P. Thouvenot, La démonstration de Furstenberg du théorème de Szemerédi sur les progressions arithmétiques, *Lect. Notes in Math.*, Springer-Verlag Berlin, **710**(1979) 221–232; *MR* **81c**:10072.

B. L. van der Waerden, Beweis einer Baudet'schen Vermutung, *Nieuw Arch. Wisk.* (2), **15**(1927) 212–216.

B. L. van der Waerden, How the proof of Baudet's conjecture was found, in *Studies in Pure Mathematics*, Academic Press, London, 1971, 251–260.

E. Witt, Ein kombinatorische Satz der Elementargeometrie, *Math. Nachr.*, **6**(1952) 261–262.

E11. Schur 问题;把整数分成无和类

Schur 证明了:如果对小于 $n!e$ 的整数用任何方式分成 n 个类,那么 $x+y=z$ 在一个类的范围内能有整数解. 令 $s(n)$是使得存在整数$[1,s(n)]$分成 n 个类的一个分划且在任何一类中该方程均无解的最大的整数. Abbott 和 Moser 得到了下界$s(n)>(89)^{n/4-c\ln n}$(对某个 c 和所有充分大的n),Abbott 和 Hanson 得到 $s(n)>c(89)^{n/4}$,这改进了 Schur 自己的估计 $s(n)\geqslant(3^n+1)/2$. 最后这个结果对 $n=1,2$ 和 3 事实上已经是最好的了,但对 n 的更大的值,这个界还是太小. Baumert 算出有 $s(4)=44$. 例如,头 44 个数可以分成 4 个无和类

$$\{1,3,5,15,17,19,26,28,40,42,44\},$$
$$\{2,7,8,18,21,24,27,33,37,38,43\},$$
$$\{4,6,13,20,22,23,25,30,32,39,41\},$$
$$\{9,10,11,12,14,16,29,31,34,35,36\}.$$

后来 Fredricksen 证明了 $s(5)\geqslant157$(作为他的例子,见 E12),这对所有后面的 Schur 数的下界 $s(n)\geqslant c(315)^{n/5}(n>5)$给出了改进.

Robert Irving 把 Schur 的上界从$\lfloor n!e\rfloor$稍许改进到$\left\lfloor n!\left(e-\frac{1}{24}\right)\right\rfloor$. 这个结果也出现在 O'Sullivan 的博士论文中(见 E28). Eugene Levine 说,这似乎是从 Jon Folkman 的结果"Ramsey 数 $R(3,3,3,3)\leqslant65$"能得出的最好的结果了. 同样地,Schinzel 注意到:认为属于 Irving 的那个结果被后者说成应属于 Earl Glen Whitehead.

用 $v=\sigma(m,n)$来记满足下述条件的最小整数 v:把$\{1,2,\cdots,v\}$分成 n 个子集的任一分化都有一个包含$a_1,\cdots,a_m$(不一定各不相同)的部分,它们满足 $a_1+\cdots+a_{m-1}=a_m$,也即 $s(n)=$

$\sigma(3,n)$. Beutelspacher 和 Brestovansky 注意到 $\sigma(m,1)=m-1$ 以及 $\sigma(2,n)=1$，并证明了 $\sigma(m,2)=m^2-m-1$. 他们展示了无 3 -和，无 6 -和以及无 7 -和分划，从而证明了 $\sigma(3,6)\geqslant 476$ 和 $\sigma(3,7)\geqslant 1430$. 于是对 $n\geqslant 7$ 有 $\sigma(3,n)\geqslant\frac{1}{2}(2859\cdot 3^{n-7}+1)$. 他们还定义并研究了算术级数的 Schur 数.

E. Szekeres 和 G. Szekeres 考虑了 Bill Sands 所称的反 Schur 问题(un-Schur problem). 把整数 $[1,n]$ 分成 3 个类的一个分划称为可接受的(admissible)，如果方程 $x+y=z$ 没有属于不同类的解 x,y,z. 对每个类的大小 $>\frac{1}{4}n$ 的情形不存在可接受的分化.

如果整数被分成 r 个类，那么必有某个类包含 3 个满足 $\frac{1}{x}+\frac{1}{y}=\frac{1}{z}$ 的不同的整数 x,y,z. 这一结论是否为真? T. C. Brown 对 $r=2$ 验证了这一结论.

参考文献

Harvey L. Abbott, PhD thesis, Univ. of Alberta, 1965.

H. L. Abbott & D. Hanson, A problem of Schur and its generalizations, *Acta Arith.*, **20**(1972) 175–187.

H. L. Abbott & L. Moser, Sum-free sets of integers, *Acta Arith.*, **11**(1966) 393–396; *MR* **34** #69.

L. D. Baumert, Sum-free sets, *Jet Propulsion Lab. Res. Summary, No. 36-10*, **1**(1961) 16–18.

Albrecht Beutelspacher & Walter Brestovansky, Generalized Schur numbers, in Combinatorial Theory, *Springer Lecture Notes in Math.*, **969**(1982) 30–38.

S. L. G. Choi, The largest sum-free subsequence from a sequence of n numbers, *Proc. Amer. Math. Soc.*, **39**(1973) 42–44; *MR* **47** #1771.

S. L. G. Choi, J. Komlós & E. Szemerédi, On sum-free subsequences, *Trans. Amer. Math. Soc.*, **212**(1975) 307–313; *MR* **51** #12769.

Paul Erdős, Some problems and results in number theory, in *Number Theory and Combinatorics* (Japan, 1984) World Sci. Publishing, Singapore, 1985, 65–87; *MR* **87g**:11003.

H. Fredricksen, Five sum-free sets, *Proc. 6th SE Conf. Graph Theory, Combin. & Comput., Congressus Numerantium* **14** Utilitas Math., 1975, 309–314.

R. W. Irving, An extension of Schur's theorem on sum-free partitions, *Acta Arith.*, **25**(1973) 55–63.

J. Komlós, M. Sulyok & E. Szemerédi, Linear problems in combinatorial number theory, *Acta Math. Acad. Sci. Hungar.*, **26**(1975) 113–121; *MR* **51** #342.
L. Mirsky, The combinatorics of arbitrary partitions, *Bull. Inst. Math. Appl.*, **11**(1975) 6–9.
J. Schönheim, On partitions of the positive integers with no x, y, z belonging to distinct classes satisfying $x+y=z$, in R. A. Mollin (ed.) Number Theory (*Proc. 1st Conf. Canad. Number Theory Assoc., Banff 1988*, de Gruyter, 1990, 515–528; *MR* **92d**:11018.
I. Schur, Über die Kongruenz $x^m+y^m\equiv z^m \bmod p$, *Jahresb. Deutsche Math.-Verein.*, **25**(1916) 114–117.
Esther & George Szekeres, Adding numbers, *James Cook Math. Notes*, **4** no. 35 (1984) 4073–4075.
W. D. Wallis, A. P. Street & J. S. Wallis, *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, Springer-Verlag, 1972.
Earl Glen Whitehead, The Ramsey number $N(3,3,3,3;2)$, *Discrete Math.*, **4**(1973) 389–396; *MR* **47** #3229.
Š. Znám, Generalisation of a number-theoretic result, *Mat.-Fyz. Časopis*, **16**(1966) 357–361.
Š. Znám, On k-thin sets and n-extensive graphs, *Math. Časopis*, **17**(1967) 297–307.

E12. 关于模的 Schur 问题

Abbott 和 Wang 考虑了一个与 Schur 问题类似的问题. 令 $t(n)$是满足下列条件的最大整数 m:存在从 1 到 m 的整数分成 n 个类的一个分划,在任何一个类中同余式

$$x+y\equiv z \bmod (m+1)$$

均无解. 显然有 $t(n)\leqslant s(n)$,其中 $s(n)$如在 Schur 问题中那样定义(E11),但对$n=1,2$ 或 3 有等式成立:$t(1)=s(1)=1$, $t(2)=s(2)=4$, $t(3)=s(3)=13$. 的确,把[1,13]分成 3 个满足无和条件的集合的仅有的 3 个分划

$$\{1,4,10,13\},\quad \{2,3,11,12\},\quad \{5,6,8,9\}.$$

(7 在 3 个集合的任何一个之中)对模 14 全都满足看起来限制更为严格的**无同余条件**(congruence-free condition),而 Baumert 的例子(E11)表明仅有一处不满足:在第二个集合中 $33+33\equiv 21 \bmod 45$. 事实上 Baumert 找到了 112 种把[1,44]分划成 4 个无和集的方法,其中有一些是模 45 的无和集,故有 $t(4)=44$. 一个例子是

$\{\pm 1, \pm 3, \pm 5, 15, \pm 17, \pm 19\}$,

$\{\pm 2, \pm 7, \pm 8, \pm 18, \pm 21\}$,

$\{\pm 4, \pm 6, \pm 13, \pm 20, \pm 22, \pm 30\}$,

$\{\pm 9, \pm 10, \pm 12, \pm 14, \pm 16\}$.

Abbott 和 Wang 得到不等式

$$f(n_1 + n_2) \geqslant 2f(n_1)f(n_2),$$

它对 $f(n) = s(n) - \frac{1}{2}$ 成立，且可导出与 Schur 对他的问题得到的同样的下界 $t(n) \geqslant (3^n + 1)/2$. 他们确实有证据表明 $t(n) = s(n)$. 此外，Fredricksen 的例子

$\pm\{1,4,10,16,21,23,28,34,40,43,45,48,54,60\}$,

$\pm\{2,3,8,9,14,19,20,24,25,30,31,37,42,47,52,65,70\}$,

$\pm\{5,11,12,13,15,29,32,33,35,36,39,53,55,56,57,59,77,79\}$,

$\pm\{6,7,17,18,22,26,27,38,41,46,50,51,75\}$,

$\pm\{44,49,58,61,62,63,64,66,67,68,69,71,72,73,74,76,78\}$

(此例表明 $s(5) \geqslant 157$)对模 158 也是无和集，故有 $t(5) \geqslant 157$，同时有 $t(n) > c(315)^{n/5}$.

Alon 和 Kleitman 把交换群的一个子集 A 称为是**无和的**(sum-free)，如果 A 中任何两个元素的和都不在 A 中，即 $(A + A) \cap A = \varnothing$. 他们证明了：每个由这样一个群的 n 个非零元素组成的集合都包含一个基数大于 $\frac{2}{7}n$ 的无和子集. 由 Rhemtulla 和 Street 的一个结果得知，$\frac{2}{7}$ 是最好可能的了，尽管对特殊的群这个数值还可以改进. 他们还证明了：任何由 n 个非零整数组成的集合都包含一个基数大于 $\frac{1}{3}n$ 的无和子集，这里 $\frac{1}{3}$ 不能被 $\frac{12}{29}$ 代替. Füredi 注意到，集合 $\{1,2,3,4,5,6,8,9,10,18\}$ 表明，此数不能被 $\frac{2}{5}$ 代替. 这里的问题是：$\frac{1}{3}$ 是最好可能的吗？

Erdös 用 $f(n)$ 记满足下列条件的最小整数：小于 n 的整数可以被分化成 $f(n)$ 个类，使得 n 不是同一个类中不同元素的和. 例

如,由于分化{1,3,4,5,9},{2,6,7,8,10},我们有 $f(11)=2$,但是 $f(12)=3$. Erdös 能证明 $f(n)<n^{1/3}/\ln n$,但他无法证明 $f(n)>n^{1/3-\epsilon}$.

参考文献

H. L. Abbott & E. T. H. Wang, Sum-free sets of integers, *Proc. Amer. Math. Soc.*, **67**(1977) 11-16; *MR* **58** #5571.

Noga Alon & Daniel J. Kleitman, Sum-free subsets, *A tribute to Paul Erdős*, Cambridge Univ. Press, Cambridge, 1990, 13–26; *MR* **92f**:11020.

H. Fredricksen, Schur numbers and the Ramsey number $N(3,3,\ldots,3;2)$, *J. Combin. Theory Ser. A*, **27**(1979), 376–377.

A. H. Rhemtulla & Anne Penfold Street, Maximum sum-free sets in elementary Abelian *p*-groups, *Canad. Math. Bull.*, **14**(1971) 73–80.

E13. 把整数分成强无和类

Turán 证明了:如果整数 $[m,5m+3]$ 以任何方式分成两个类,那么方程 $x+y=z$ 至少在其中的一个类中有 $x\neq y$ 的解,而且这一结果对整数 $[m,5m+2]$ 不真. $[m,5m+2]$ 分划成两个无和集的惟一性被 Znám 所证明.

Turán 还考虑了 x,y 不一定互不相同时的问题. 定义 $s(m,n)$ 是满足如下条件的最小整数 s:无论怎样将区间 $[m,m+s]$ 分化成 n 个类,总有一个类包含有 $x+y=z$ 的一个解. 对应于第一个问题他得到的结果是 $s(m,2)=4m$. 显然有 $s(1,n)=s(n)-1$,这里 $s(n)$ 定义在 E11 中,而 Irving 的结果蕴含 $s(m,n)\leqslant m\left\lfloor -n!\left(e-\frac{1}{24}\right)-1\right\rfloor$. Abbott 和 Znám(见 E11)独立地发现了 $s(m,n)\geqslant 3s(m,n-1)+m$,从而有 $s(m,n)\geqslant m(3^n-1)/2$.

Abbott 和 Hanson 称一个类是强无和的(strongly sum-free),如果它既不包含方程 $x+y=z$ 的解,也不包含方程 $x+y+1=z$ 的解. 他们证明了:如果 $r(n)$ 是使得区间 $[1,r]$ 无论如何分化成 n 个类,都有一个类包含有这样一个解的最小的 r,那么

$$r(m+n)\geqslant 2r(n)s(m)-r(n)-s(m)+1.$$

他们用这一结果改进了 $s(m,n)$ 的下界，现在，他们的方法和 Fredericksen 的例子合起来给出 $s(m,n) > cm(315)^{n/5}$.

参考文献

Š. Znám, Megjegyzések Turán Pál egy publikálatlan eredményéhez, *Mat. Lapok*, **14** (1963) 307–310.

E14. Rado 对 van der Waerden 问题和 Schur 问题的推广

Rado 考虑过 van der Waerden 以及 Schur 问题的若干推广. 例如他证明了：对任何自然数 a, b, c，存在一个数 u，使得无论怎样将数 $[1, u]$ 分化成两个类，至少在其中一个类中有 $ax + by = cz$ 的一个解. 他给出了 u 的值，但是如同在 Schur 原来的问题中那样，这里给出的并非是最好可能的结果. 例如对 $2x + y = 5z$，定理给出 $u = 20$，但它甚至对 $u = 15$ 也仍然是对的，虽然对 u 的更小的值未必为真：集合

$$\{1,4,5,6,9,11,14\}, \quad \{2,3,7,8,10,12,13\}$$

中无论哪一个都不包含 $2x + y = 5z$ 的解. 如果允许取 3 个集合，则 45 是 u 的最小值，这是因为如下 3 个集合

$$\{1,4,5,6,9,11,14,16,19,20,21,24,26,29,31,34,36,39,41,44\},$$
$$\{2,3,7,8,10,12,13,15,17,18,22,23,27,28,32,33,37,38,42,43\},$$
$$\{6,7,8,9,25,30,35,40\}$$

就包含了 $[1,44]$ 中所有的数，甚至 6,7,8,9 还重复了.

Rado 把方程 $\sum a_i x_i = 0$（其中诸 a_i 是非零整数）称为是 n-重正则的（n-fold regular），如果存在一个数 $u(n)$（我们可以假设它是最小的），使得无论怎样把区间 $[1, u(n)]$ 分化成 n 个类，都至少有一个类包含该方程的一个解. 他把方程称为是正则的（regular），如果对所有 n 它都是 n-重正则的. 他证明了：一个方程是正则的，仅当对 a_i 的某个子集有 $\sum a_j = 0$. 例如，如果 $a_1 = a_2 = 1$ 且 $a_3 = -1$，我们就对 Schur 原来的问题得到 $u(n) = s(n)$.

Salié 和 Abbott 考虑了求 $u(n)$ 的下界这个问题，作为参考请见 E10 和 E11.

与 $a_1=2, a_2=1, a_3=-5$ 对应的例子不是正则的，这是因为，虽然我们看到它既是 2-重正则的又是 3-重正则的，但它不是 4-重正则的. 因为，把每个数 $5^k l$（这里 $5 \nmid l$）按照 k 是偶数还是奇数以及 $l \equiv \pm 1$ 还是 $\pm 2 \bmod 5$ 划分到 4 个类中的一个类中去. 可以验证，这 4 个类中无论哪个类都不含有 $2x+y=5z$ 的解.

Rado 问：对每个 k 是否存在一个方程，它是 k-正则的，但不是 $(k+1)$-正则的？

对方程 $2x_1+x_2=2x_3$ 和 $x_1+x_2+x_3=2x_4$, Salié, Abbott 以及 Abbott 和 Hanson 相继得到了更好的下界，最后分别得到 $u(n)>c(12)^{n/3}$ 和 $c(10)^{n/3}$.

Vera Sós 要求 $[1,n]$ 的使得 Rado 方程在其中没有解的那种子集的最大范围. 例如，如果 $a_1=a_2=1$ 且 $a_3=-2$，则答案在区间 $[n\exp(-\sqrt{\ln n}), n/(\ln n)^\alpha]$ 之中. 如果 $a_1=a_2=1$ 且 $a_3=a_4=-1$，我们就得到一个 Sidon 集合（与 C9 比较），而此时答案是 $\approx \sqrt{n}$. 如果 $a_1=a_2=1$ 且 $a_3=-1$，则答案是 $n/2$. 已知更一般地有答案 $o(n)$（正好当 $x_1=x_2=\cdots=1$ 是 Rado 方程的一个解时）. 这个答案能与 $n_\alpha\left(\frac{1}{2}<\alpha<1\right)$ 作比较吗？

请将问题 E10～14 和 C14～16 作比较.

参 考 文 献

Walter Deuber, Partitionen und lineare Gleichungssysteme, *Math. Z.*, **133** (1973) 109–123.

R. Rado, Studien zur Kombinatorik, *Math. Z.*, **36**(1933) 424–480.

E. R. Williams, M.Sc. thesis, Memorial University, 1967.

E15. Göbel 的递归公式

很长一段时间里 F. Göbel 注意到：递归公式 $x_0=1$,

$$x_n = (1 + x_0^2 + x_1^2 + \cdots + x_{n-1}^2)/n, \quad n = 1,2,\cdots$$

(或者表为对 $n>0$ 有 $(n+1)x_{n+1}=x_n(x_n+n)$)产生出整数

$$x_1 = 2,3,5,10,28,154,3520,1551880,267593772160,\cdots,$$

但是 Hendrik Lenstra 发现 x_{43}不是整数!

用立方代替平方得到的相应的序列要一直到 x_{89}才出现非整数. Henry Ibstedt 对各种幂以及不同的初值 x_0 做了进一步的计算. 下面的表指出了序列中第一个非整数元素的序号

k	2	3	4	5	6	7	8	9	10	11
$x_1=2$	43	89	97	214	19	239	37	79	83	239
$x_1=3$	7	89	17	43	83	191	7	127	31	389
$x_1=4$	17	89	23	139	13	359	23	158	41	239
$x_1=5$	34	89	97	107	19	419	37	79	83	137
$x_1=6$	17	31	149	269	13	127	23	103	71	239
$x_1=7$	17	151	13	107	37	127	37	103	83	239
$x_1=8$	51	79	13	214	13	239	17	163	71	239
$x_1=9$	17	89	83	139	37	191	23	103	23	169
$x_1=10$	7	79	23	251	347	239	7	163	41	239
$x_1=11$	34	601	13	107	19	478	37	79	31	389

Raphael Robinson 注意到,与 Göbel 的序列形成对照的是,下述序列

$$x_n x_{n-k} = a x_{n-p} x_{n-k+p} + b x_{n-q} x_{n-k+q} + c x_{n-r} x_{n-k+r}$$

似乎从初始值 $x_0=x_1=\cdots=x_k=1$ 开始对任何整数 $a\geqslant 0, b\geqslant 0, c\geqslant 0, p\geqslant 1, q\geqslant 1, r\geqslant 1$ 都取整数值,这里 k 满足 $p+q+r=k$.

参考文献

David Gale, Mathematical Entertainments, *Math. Intelligencer*, **13**(1991) No. 1, 40–43.

Henry Ibstedt, Some sequences of large integers, *Fibonacci Quart.*, **28**(1990) 200–203; *MR* **91h**:11011.

Janice L. Malouf, An integer sequence from a rational recursion, *Discrete Math.*, **110**(1992) 257-261.

Raphael M. Robinson, Periodicity of Somos sequences, *Proc. Amer. Math. Soc.*, **116**(1992) 613–619; *MR* **93a**:11012.

Michael Somos, Problem 1470, *Crux Mathematicorum*, **15**(1989) 208.

E16. Collatz 序列

当 L. Collatz 还是一个学生时，他问道：由 $a_{n+1}=a_n/2$（当 a_n 为偶数时）和 $a_{n+1}=3a_n+1$（当 a_n 为奇数时）定义的序列，除了圈 4,2,1,4…（图 16）以外，是否都是树形结构的（它的含意是指从任何一个整数 a_1 开始，都有一个 n 使 $a_n=1$）？这一猜想已对所有 $a_1\leqslant 2\cdot 10^{12}$ 和许多大数作了检验. Eliahou 证明了：任何非平凡的

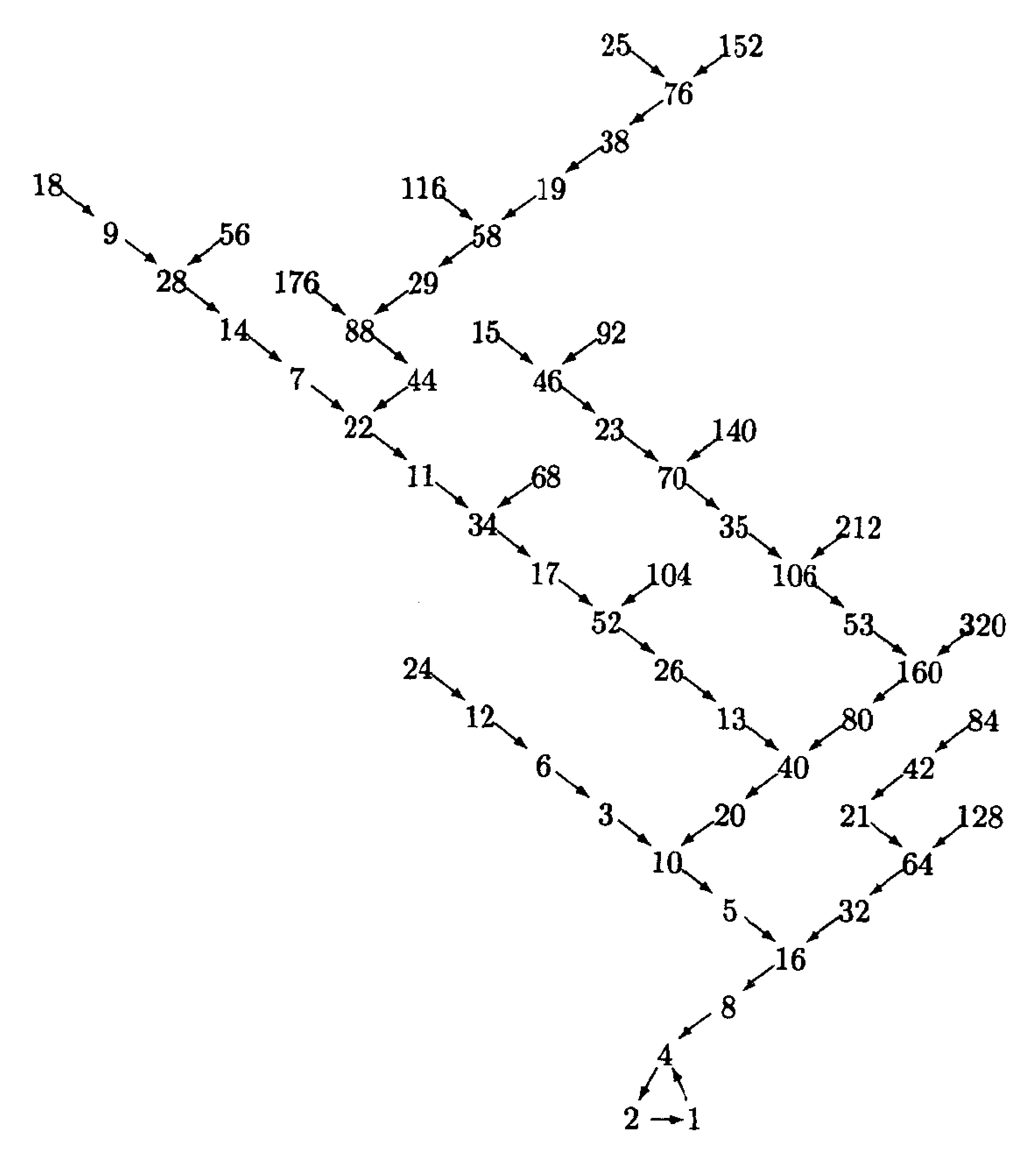


图 16　Collatz 序列是树形的吗？

圈的周期至少是 17087915.

如果用 $3a_n-1$ 代替 $3a_n+1$(如果我们允许取负整数的话)，那么很可能任何序列都以下面几个圈中的一个作为结束：

$$\{1,2\},\{5,14,7,20,10\}$$

或者

$$\{17,50,25,74,37,110,55,164,82,41,122,\\ 61,182,91,271,136,68,34\}.$$

这一结论对所有 $a_1\leqslant 10^8$ 为真.

更为一般地，David Kay 和其他的人用 $a_{n+1}=a_n/p$(如果 $p\mid a_n$)和 $a_{n+1}=qa_n+r$(如果 $p\nmid a_n$)定义了序列，并且问是否存在数 p,q,r，使得此问题可以解决？对$(p,q,r)=(2,5,1)$或$(2,7,1)$，任何即使琢磨不定的序列也都将会迅速增长，这似乎是相当合情合理的，但是要证明这样的结论看起来和原来的问题一样困难. 现有的文献极多，我们敦请未来的解题者们赶紧仔细研究 Lagarias 的论著.

定义 $f(n)$是 $3n+1$ 的最大奇数因子. Zimian 问：

$$\prod_{i=1}^{m} n_i = \prod_{i=1}^{m} f(n_i)$$

是否对任何(多重)整数集合$\{n_i\}$($n_i>1$)都成立？Erdös 发现

$$65\cdot7\cdot7\cdot11\cdot11\cdot17\cdot17\cdot13$$
$$=49\cdot11\cdot11\cdot17\cdot17\cdot13\cdot13\cdot5.$$

整数 n 称为是自我包含的(self-contained)，如果对某个 $k\geqslant 1$，n 整除 $f^k(n)$. 如果它发生了，且 Collatz 序列 $n^*=f^k(n)/n$ 达到 1，那么集合

$$\{n,f(n),\cdots,f^{k-1}(n),n^*,f(n^*),\cdots,1\}$$

就是如上所说的一个集合. 对 $n\leqslant 10^4$ 用计算机搜索得到 5 个自我包含的整数:31,83,293,347 和 671.

这些映射不是一对一的，你无法追踪序列的前面的项，因为映射的逆常常不是惟一的.

参考文献

J.-P. Allouche, Sur la conjecture de "Syracuse-Kakutani-Collatz," *Séminaire de Théorie des Nombres*, 1978/79, Exp. No. 9, Talence, 1979; *MR* **81g**:10014.

David Applegate & Jeffery C. Lagarias, Density bounds for the $3x+1$ problem, Abstract 882-11-10, *Abstracts Amer. Math. Soc.*, **14**(1993) 414.

Michael Beeler, William Gosper & Rich Schroeppel, Hakmem, Memo 239, Artificial Intelligence Laboratory, M.I.T., 1972, p. 64.

Daniel J. Bernstein, A noniterative 2-adic statement of the $3N+1$ conjecture, *Proc. Amer. Math. Soc.*, (1993).

David Boyd, Which rationals are ratios of Pisot sequences? *Canad. Math. Bull.*, **28**(1985) 343–349; *MR* **86j**:11078.

R. E. Crandall, On the "$3x+1$" problem, *Math. Comput.*, **32**(1978) 1281–1292; *MR* **58** #494.

J. L. Davidson, Some comments on an iteration problem, Proc. 6th Manitoba Conf. Numerical Math., 1976, *Congressus Numerantium*, **18**(1977) 155–159.

S. Eliahou, The $3x+1$ problem: new lower bounds on nontrivial cycle lengths, *Discrete Math.*, **118**(1993) 45–56.

C. J. Everett, Iteration of the number-theoretic function $f(2n) = n$, $f(2n+1) = 3n+2$, *Advances in Math.*, **25**(1977) 42–45; *MR* **56** #15552.

P. Filipponi, On the $3n+1$ problem: something old, something new, *Rend. Mat. Appl.*(7) **11**(1991) 85–103; *MR* **92i**:11031.

L. E. Garner, On the Collatz $3n+1$ algorithm, *Proc. Amer. Math. Soc.*, **82**(1981) 19–22; *MR* **82j**:10090.

Lynn E. Garner, On heights in the Collatz $3n+1$ problem, *Discrete Math.*, **55**(1985) 57–64; *MR* **86j**:11005.

E. Heppner, Eine Bemerkung zum Hasse-Syracuse-Algorithmus, *Arch. Math. (Basel)*, **31**(1977/79) 317–320; *MR* **80d**:10007.

I. N. Herstein & I. Kaplansky, *Matters Mathematical*, 2nd ed., Chelsea, 1978, pp. 44–45.

David C. Kay, *Pi Mu Epsilon J.*, **5**(1972) 338.

I. Korec & Š. Znám, A note on the $3x+1$ problem, *Amer. Math. Monthly*, **94**(1987) 771–772.

I. Krasikov, How many numbers satisfy the $3x+1$ conjecture? *Internat. J. Math. Math. Sci.*, **12**(1989) 791–796; *MR* **90k**:11013.

Jeffrey C. Lagarias, The $3x+1$ problem and its generalizations, *Amer. Math. Monthly*, **92**(1985) 3–23, *MR* **86i**:11043.

Jeffrey C. Lagarias, The set of rational cycles for the $3x+1$ problem, *Acta Arith.*, **56**(1990) 33–53, *MR* **91i**:11024.

J. C. Lagarias, H. A. Porta & K. B. Stolarsky, Asymmetric tent map expansions I: eventually periodic points, *J. London Math. Soc.*, **47**(1993) 542–556.

Jeffrey C. Lagarias & A. Weiss, The $3x+1$ problem: two stochastic models, *Ann. Appl. Probab.*, **2**(1992) 229–261.

K. R. Matthews & A. M. Watts, A generalization of Hasse's generalization of the

Syracuse algorithm, *Acta Arith.*, **43**(1984) 167–175; *MR* **85i**:11068.

K. R. Matthews & A. M. Watts, A Markov approach to the generalized Syracuse algorithm, *Acta Arith.*, **45**(1985) 29–42; *MR* **87c**:11071.

Herbert Möller, Über Hasses Verallgemeinerung der Syracuse-Algorithmus (Kakutani's problem), *Acta Arith.*, **34**(1978) 219–226; *MR* **57** #16246.

Helmut Müller, Das "$3n+1$"-Problem, *Mitt. Math. Ges. Hamburg*, **12**(1991) 231–251.

Daniel A. Rawsthorne, Imitation of an iteration, *Math. Mag.*, **58**(1985) 172–176; *MR* **86i**:40001.

J. W. Sander, On the $(3N+1)$-conjecture, *Acta Arith.*, **55**(1990) 241–248; *MR* **91m**:11052.

J. Shallit, The "$3x+1$" problem and finite automata, *Bull. Europ. Assoc. Theor. Comput. Sci.*, **46**(1991) 182–185.

Ray P. Steiner, On the "$Qx+1$ problem", Q odd, *Fibonacci Quart.*, **19**(1981) 285–288; II, 293–296.

Riho Terras, A stopping time problem on the positive integers, *Acta Arith.*, **30**(1976) 241–252; *MR* **58** #27879 (and see **35**(1979) 100–102; *MR* **80h**:10066)

Ilan Vardi, Computational Recreations in *Mathematica*©, Addison-Wesley, Redwood City CA, 1991, Chap. 7.

G. Venturini, Iterates of number-theoretic functions with periodic rational coefficients (generalization of the $3x+1$ problem), *Stud. Appl. Math.* **86**(1992) 185–218; *MR* **93b**:11102.

Stan Wagon, The Collatz problem, *Math. Intelligencer*, **7**(1985) 72–76.

Masaji Yamada, A convergence proof about an integral sequence, *Fibonacci Quart.*, **18**(1980) 231–242; see *MR* **82d**:10026 for errors.

E17. 置换序列

在**置换序列**(permutation sequence)这一情形,尽管问题同样困难,但情势有所不同. 一个简单的例子(可能是 Collatz 原来问题的反问题,见 E16 和提到的 Lagarias 的文章)是

$$a_{n+1}=3a_n/2\quad(\text{若 } a_n \text{ 为偶数}),$$
$$a_{n+1}=\lfloor(3a_n+1)/4\rfloor\quad(\text{若 } a_n \text{ 为奇数}),$$

或者,可能更为明确地是表述成

$$2m\to3m,\quad 4m-1\to3m-1,\quad 4m+1\to3m+1,$$

由此可以清楚地看出其逆运算也能顺利施行. 因此它产生的结构仅由不相交的圈和双无穷链组成. 不知道它们中每一种是有有限

多个还是无穷多个？甚至也不知道是否有一个无穷的链存在？猜想仅有的圈是{1}，{2,3}，{4,6,9,7,5}和

{44,66,99,74,111,83,62,93,70,105,79,59}.

Mike Guy 借助于一台名为 TITAN 的计算机证明了：任何别的圈都有大于 320 的周期. 那么包含数 8 的序列情况又如何呢?

…,97,73,55,41,31,23,17,13,10,15,11,8,

12,18,27,20,30,45,34,51,38,57,43,32,48,72,…

诸数

8,14,40,64,80,82,104,136,172,184,188,242,256,274,280,296,352,368,382,386,424,472,496,526,530,608,622,638,640,652,670,688,692,712,716,752,760,782,784,800,814,824,832,960,878,904,910,932,964,980,…

中的每一个数是否都属于一个单独分开的序列?

有一些颇为吸引人的悖论：如果现有的是个偶数，你就“向前”走，乘以 3/2；如果它是奇数，则乘以大约 3/4——这样得到一个公比是 $3/\sqrt{8}\approx1.060660172$ 的不稳定的“伪几何级数”. 另一方面，如果现有的数是 3 的倍数，你就“向后”退，乘以 2/3，否则的话就乘以大约 4/3——这样得到一个公比是 $32^{1/3}/3\approx1.058267368$ 的“伪几何级数”. 这两个数应该互为倒数！我们对处处不可微的函数有一种离散的类似. 右“导数”是正的，左“导数”是负的. 注意，当“向前”走时，接在偶数后面那个数是 3 的倍数——有一半数是 3 的倍数！

参 考 文 献

J. H. Conway, Unpredictable iterations, in *Proc. Number Theory Conf.*, Boulder CO, 1972, 49–52; *MR* **52** #13717.

David Gale, Mathematical Entertainments, *Math. Intelligencer*, **13**(1991) No. 3, 53–55.

G. Venturini, Iterates of number theoretic functions with periodic rational coefficients (generalization of the $3x+1$ problem), *Stud. Appl. Math.*, **86**(1992) 185–218.

E18. Mahler 的 Z-数

Mahler 考虑了下面的问题:给定任何实数 α,令 r_n 为$\alpha(3/2)^n$ 的分数部分. 是否存在对所有 n 都满足 $0\leqslant r_n<\frac{1}{2}$ 的所谓 **Z-数** (Z-number)呢? 可能并不存在. Mahler 指出,在每一对相邻整数中至多有一个这样的数,且对足够大的 x,小于 x 的 Z-数的个数至多有 $x^{0.7}$个. Flatto 改进了 Mahler 的结果,但是这一问题仍未获得解决.

一个类似的问题是:是否存在有理数 $r/s(s\neq1)$,使对所有 n,$\lfloor(r/s)^n\rfloor$都是奇数呢? Tijdeman 证明了:对每个奇整数 $r>3$,存在实数 α,使对所有 n,$\alpha(r/2)^n$ 的分数部分都在$\left[0,\frac{1}{2}\right)$中.

Littlewood 有一次曾说起过:不知道 e^n 的分数部分是否趋向于0(当 $n\to\infty$时)?

参考文献

Leopold Flatto, *Z*-numbers and *β*-transformations, *Symbolic Dynamics and its Applications, Contemporary Math.*, **135**, Amer. Math. Soc., 1992, 181–201.

K. Mahler, An unsolved problem on the powers of 3/2, *J. Austral. Math. Soc.*, **8**(1968) 313–321; *MR* **37** #2694.

R. Tijdeman, Note on Mahler's $\frac{3}{2}$-problem, *Kongel. Norske Vidensk. Selsk. Skr.*, **16**(1972) 1–4.

E19. 一个分数的幂的整数部分能无穷多次取素数值吗?

Forman 和 Shapiro 证明了,有无穷多个形如$\lfloor(4/3)^n\rfloor$的整数,也有无穷多个形如$\lfloor(3/2)^n\rfloor$的合数. A. L. Whiteman 猜想:这两个序列的每一个也都包含无穷多个素数. 他们的方法对其他的有理数似乎不起作用.

参考文献

W. Forman & H. N. Shapiro, An arithmetic property of certain rational powers, *Comm. Pure Appl. Math.*, **20**(1967) 561-573; *MR* **35** #2852.

E20. Davenport-Schinzel 序列

从 n 个字母的字母表$[1,n]$出发来构造一个序列，使得其中没有直接的重复$\cdots aa\cdots$，也没有长度大于 d 的交错的子序列

$$\cdots a\cdots b\cdots a\cdots b\cdots.$$

用 $N_d(n)$来记任何这样的序列的最大长度，那么有这种长度的一个序列就是一个 Davenport-Schinzel 序列(Davenport-Schinzel sequence). 问题是要确定所有的 D-S 序列，特别是要求出 $N_d(n)$. 我们只需要考虑正规的(normal)序列，所谓正规序列，就是字母表中每个整数的首次出现要在其中每个更小的数的首次出现之后.

序列 12131323，12121213131313232323 和

$$1\ 2\ 1\ 3\ 1\ 4\ 1\cdots 1\ \overline{n-1}\ 1\ \overline{n-1}\ \overline{n-2}\cdots 3\ 2\ n\ 2\ n\ 3\ n\cdots n\ \overline{n-1}\ n$$

表明 $N_4(3)\geqslant 8$，$N_8(3)\geqslant 20$，且 $N_4(n)\geqslant 5n-8$. Davenport 和 Schinzel 证明了 $N_1(n)=1$，$N_2(n)=n$，$N_3(n)=2n-1$；又有 $N_4(n)=O(n\ln n/\ln\ln n)$，$\lim N_4(n)/n\geqslant 8$. 他还和 J. H. Conway 一起证明了 $N_4(lm+1)\geqslant 6lm-m-5l+2$，因此有$N_4(n)=5n-8(4\leqslant n\leqslant 10)$. Z. Kolba 证明了 $N_4(2m)\geqslant 11m-13$，而 Mills 则对$n\leqslant 21$得到了 $N_4(n)$的值. 例如，序列

abacadaeafafedcbgbhbhgcicigdjdjgekekgkjihflflhliljlkl

是 $N_4(12)=53$ 的证明的一部分.

Roselle 和 Stanton 是将 n(而不是 d)加以固定，对此得到 $N_d(2)=d$，$N_d(3)=2\lfloor 3d/2\rfloor-4(d>3)$，$N_d(4)=2\lfloor 3d/2\rfloor+3d-13(d>4)$以及 $N_d(5)=4\lfloor 3d/2\rfloor+4d-27(d>5)$. 尽管 Peterkin 注意到最后这个括号应该是$(d>6)$，这是因为有 $N_6(5)=34$. Roselle和Stanton还证明了：长为$N_{2d+1}(5)$的正规的D-S序

列是惟一的，且长为 $N_{2d+1}(4)$和 $N_{2d}(5)$的正规的 D-S 序列恰有两个. Peterkin 展示了 56 个长为$N_5(6)=29$的 D-S 序列，并证明了$N_5(n)\geqslant 7n-13(n>5)$以及 $N_6(n)\geqslant 13n-32(n>5)$.

表 8　$N_d(n)$的值

d \ n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
3	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41
4	1	4	8	12	17	22	27	32	37	42	47	53	58	64	69	75	81	86	92	98	104
5	1	5	10	16	22	29															
6	1	6	14	23	34																
7	1	7	16	28	41																
8	1	8	20	35	53																
9	1	9	22	40	61																
10	1	10	26	47	73																

Rennie 和 Dobson 给出 $N_d(n)$的形如

$$(nd-3n-2d+7)N_d(n)$$
$$\leqslant n(d-3)N_d(n-1)+2n-d+2 \quad (d>3)$$

的上界，从而对 $d=4$ 推广了 Roselle 和 Stanton 的结果.

Szemerédi 证明了 $N_d(n)<c_d n\log^* n$，这里 $\log^* n$ 是一个增长得很慢的函数，指数函数的最小迭代次数需要超过 n. 新近的工作(主要是由 Sharir 所做的)证实：$N_d(n)$的阶是 $\Theta(n\alpha(n))$，这里 $\alpha(n)$是 Akermann 函数的反函数，它增长得令人难以置信的慢. 有关的细节请参看 Agarwal, Sharir 和 Shor 的论文.

参 考 文 献

P. K. Agarwal, M. Sharir & P. Shor, Sharp upper and lower bounds on the length of general Davenport-Schinzel sequences, *J. Combin. Theory Ser. A*, **52**(1989) 228-274; *MR* **90m**:11034.

H. Davenport & A. Schinzel, A combinatorial problem connected with differential equations, *Amer. J. Math.*, **87**(1965) 684-694; II, *Acta Arith.*, **17**(1970/71) 363-372; *MR* **32** #7426; **44** #2619.

Annette J. Dobson & Shiela Oates Macdonald, Lower bounds for the lengths

of Davenport-Schinzel sequences, *Utilitas Math.*, **6**(1974) 251–257; *MR* **50** #9781.
Z. Füredi & P. Hajnal, Davenport-Schinzel theory of matrices, *Discrete Math.*, **103**(1992) 233–251.
D. Gardy & D. Gouyou-Beauchamps, Enumerating Davenport-Schinzel sequences, *RAIRO Inform. Théor. Appl.* **26**(1992) 387–402.
S. Hart & M. Sharir, Nonlinearity of Davenport-Schinzel sequences and of generalized path compression schemes, *Combinatorica*, **6**(1986) 151–177.
P. Komjáth, A simplified construction of nonlinear Davenport-Schinzel sequences, *J. Combin. Theory Ser. A*, **49**(1988) 262–267.
W. H. Mills, Some Davenport-Schinzel sequences, *Congress. Numer.* **9**, Proc. 3rd Manitoba Conf. Numer. Math., 1973, pp. 307–313; *MR* **50** #135.
W. H. Mills, On Davenport-Schinzel sequences, *Utilitas. Math.* **9**(1976) 87–112; *MR* **53** #10703.
R. C. Mullin & R. G. Stanton, A map-theoretic approach to Davenport-Schinzel sequences, *Pacific J. Math.*, **40**(1972) 167–172; *MR* **46** #1745.
C. R. Peterkin, Some results on Davenport-Schinzel sequences, *Congress. Numer.* **9**, Proc. 3rd Manitoba Conf. Numer. Math., 1973, pp. 337–344; *MR* **50** #136.
B. C. Rennie & Annette J. Dobson, Upper bounds for the lengths of Davenport-Schinzel sequences, *Utilitas Math.*, **8**(1975) 181–185; *MR* **52** #13624.
D. P. Roselle, An algorithmic approach to Davenport-Schinzel sequences, *Utilitas Math.*, **6**(1974) 91–93; *MR* **50** #9780.
D. P. Roselle & R. G. Stanton, Results on Davenport-Schinzel sequences, *Congress. Numer.* **1** Proc. Louisiana Conf. Combin. Graph Theory, Comput., (1970) 249–267; *MR* **43** #68.
D. P. Roselle & R. G. Stanton, Some properties of Davenport-Schinzel sequences, *Acta Arith.*, **17**(1970/71) 355–362; *MR* **44** #1641.
M. Sharir, Almost linear upper bounds on the length of generalized Davenport-Schinzel sequences, *Combinatorica*, **7**(1987) 131–143.
Micha Sharir, Improved lower bounds on the length of Davenport-Schinzel sequences, *Combinatorica*, **8**(1988) 117–124; *MR* **89j**:11024.
R. G. Stanton & D. P. Roselle, A result on Davenport-Schinzel sequences, *Combinatorial Theory and its Applications*, Proc. Colloq., Balatonfüred, 1969, North-Holland, 1970, pp. 1023–1027; *MR* **46** #3324.
R. G. Stanton & P. H. Dirksen, Davenport-Schinzel sequences, *Ars Combin.*, **1**(1976) 43–51; *MR* **53** #13106.
E. Szemerédi, On a problem of Davenport and Schinzel, *Acta Arith.*, **25** (1973/74) 213–224; *MR* **49** #244.

E21. Thue 序列

Thue 证明了，存在无穷多个用 3 个符号作成的序列，它们不包含两个完全相同的连续片段，又存在无穷多个用 2 个符号作成的序列，它们不包含 3 个完全相同的连续片段，其他许多人又重新

发现了这些结果.

代替完全相同的片段,如果我们改为要求避免互为对方的排列的那种连续的片段,Justin 构造了一个用两个符号做成的序列,它没有 5 个互为对方的排列的连续片段,Pleasants 构造了一个由 5 个符号做成的序列,它没有两个这样的连续片段. Dekking 解决了问题(2,4)和(3,3),但是把(4,2)这一情形描写成了一个有趣的未解决的问题. 是否有一个用 4 个符号做成的序列,它没有互为对方的排列的连续片段呢?

参考文献

S. Arshon, Démonstration de l'éxistence des suites asymétriques infinies (Russian. French summary), *Mat. Sb.*, **2**(44)(1937) 769–779.

C. H. Braunholtz, Solution to Problem 5030 [1962,439], *Amer. Math. Monthly*, **70**(1963) 675–676.

T. C. Brown, Is there a sequence on four symbols in which no two adjacent segments are permutations of one another? *Amer. Math. Monthly*, **78**(1971) 886–888.

Richard A. Dean, A sequence without repeats on x, x^{-1}, y, y^{-1}, *Amer. Math. Monthly*, **72**(1965) 383–385.

F. M. Dekking, On repetitions of blocks in binary sequences, *J. Combin. Theory Ser. A*, **20**(1976) 292–299.

F. M. Dekking, Strongly non-repetitive sequences and progression-free sets, *J. Combin. Theory Ser. A*, **27**(1979) 181–185.

R. C. Entringer, D. E. Jackson & J. A. Schatz, On non-repetitive sequences, *J. Combin. Theory Ser. A*, **16**(1974) 159–164.

P. Erdős, Some unsolved problems, *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, **6**(1961) 221–254, esp. p. 240.

A. A. Evdokimov, Strongly asymmetric sequences generated by a finite number of symbols, *Dokl. Akad. Nauk SSSR*, **179**(1968) 1268–1271; *Soviet Math. Dokl.*, **7**(1968) 536–539.

Earl Dennet Fife, Binary sequences which contain no BBb, PhD thesis, Wesleyan Univ., Middletown CT, 1976.

D. Hawkins & W. E. Mientka, On sequences which contain no repetitions, *Math. Student*, **24**(1956) 185–187; *MR* **19**, 241.

G. A. Hedlund, Remarks on the work of Axel Thue on sequences, *Nordisk Mat. Tidskr.*, **15**(1967) 147–150; *MR* **37** #4454.

G. A. Hedlund & W. H. Gottschalk, A characterization of the Morse minimal set, *Proc. Amer. Math. Soc.*, **16**(1964) 70–74.

J. Justin, Généralisation du théorème de van de Waerden sur les semi-groupes répétitifs, *J. Combin. Theory Ser. A*, **12**(1972) 357–367.

J. Justin, Semi-groupes répétitifs, *Sém. IRIA, Log. Automat.*, 1971, 101–105, 108; *Zbl.* 274.20092.

J. Justin, Characterization of the repetitive commutative semigroups, *J. Algebra*, **21**(1972) 87–90; *MR* **46** #277. **12**(1972) 357–367.

John Leech, A problem on strings of beads, *Math. Gaz.*, **41**(1957) 277–278.

W. F. Lunnon & P. A.B. Pleasants, Characterization of two-distance sequences, *J. Austral. Math. Soc. Ser. A*, **53**(1992) 198–218; *MR* **93h**:11027.

Marston Morse, A solution of the problem of infinite play in chess, *Bull. Amer. Math. Soc.*, **44**(1938) 632.

Marston Morse & Gustav A. Hedlund, Unending chess, symbolic dynamics and a problem in semigroups, *Duke Math. J.*, **11**(1944) 202.

P. A. B. Pleasants, Non-repetitive sequences, *Proc. Cambridge Philos. Soc.*, **68**(1970) 267–274.

Helmut Prodinger & Friedrich J. Urbanek, Infinite 0-1 sequences without long adjacent identical blocks, *Discrete Math.*, **28**(1979) 277–289.

H. E. Robbins, On a class of recurrent sequences, *Bull. Amer. Math. Soc.*, **43**(1937) 413–417.

A. Thue, Über unendliche Zeichenreihen, *Norske Vid. Selsk. Skr. I Mat.-Nat. Kl. Christiana*, 1906, No. 7, 1–22.

A. Thue, Über die gegensetige Lage gleicher Teile gewisser Zeichenreihen, *Norske Vid. Selsk. Skr. I Mat.-Nat. Kl. Christiana*, 1912, No. 1, 1–67.

E22. 把所有排列作为子序列的圈和序列

Hansraj Gupta 要求对 $n \geqslant 2$ 求出最小正整数 $m=m(n)$，使得存在一个正整数的圈 $a_1, a_2, \cdots, a_m$（每个数都 $\leqslant n$），对至少一个 $j(1 \leqslant j \leqslant m)$，前 n 个自然数的任一给定的排列都作为

$$a_j, a_{j+1}, \cdots, a_1, a_2, \cdots, a_{j-1}$$

的一个子序列出现（不一定是相连的）. 例如对 $n=5$ 来说，1,2,3,4,5,4,3,2,1,5,4,5 就是这样一个圈，所以 $m(5) \leqslant 12$. 他猜想有 $m(n) \leqslant \lfloor n^2/2 \rfloor$.

Motzkin 和 Straus 利用了直尺函数(ruler function)，也即整除 k 的 2 的最高幂的指数，例如 $n=5, 1 \leqslant k \leqslant 31$，

$$1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,$$

$$1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,$$

但是这没有用到循环选择，这仅仅给出了 $m(n) \leqslant 2^n - 1$.

E23. 用算术级数覆盖整数

如果 S 是 n 个算术级数的并集，每个算术级数的公差都 $\geqslant k$，其中 $k \leqslant n$，Crittenden 和 Vanden Eynden 猜想：只要 S 包含 $\leqslant k2^{n-k+1}$ 的那些正整数，那么他就包含所有的正整数. 如果此猜想为真，那么它已经是最好可能的结果了. 他们对 $k=1$ 和 2 证明了这一猜想，而 Simpson 则对 $k=3$ 给出了证明.

参 考 文 献

R. B. Crittenden & C. L. Vanden Eynden, Any n arithmetic progressions covering the first 2^n integers covers all integers, *Proc. Amer. Math. Soc.*, **24**(1970) 475–481.

R. B. Crittenden & C. L. Vanden Eynden, The union of arithmetic progressions with differences not less than k, *Amer. Math. Monthly*, **79**(1972) 630.

R. Jamie Simpson, Ph.D. thesis, Univ. of Adelaide, 1985.

E24. 无理性序列

Erdös 和 Straus 称一个正整数的序列 $\{a_n\}$ 是**无理性序列**(irrationality sequence)，如果对所有整数序列 $\{b_n\}$，$\sum 1/a_nb_n$ 都是无理数. 哪些是无理性序列呢？请找出一些有意思的例子. 如果 $\limsup(\log_2 \ln a_n)/n > 1$，这里的 log 是以 2 为底的对数，那么 $\{a_n\}$ 是一个无理性序列. 注意：$\{n!\}$ 不是无理性序列，因为 $\sum 1/n!(n+2) = \frac{1}{2}$. Erdös 证明了 $\{2^{2^n}\}$ 是一个无理性序列. 序列 2,3,7,43,1807,…(这里 $a_{n+1} = a_n^2 - a_n + 1$)不是无理性序列，这是因为我们可以取 $b_n = 1$，从而该序列的倒数之和为 1，但是关于隔项取得的序列 2,7,1807,…呢？

参考文献

P. Erdős, On the irrationality of certain series, *Nederl. Akad. Wetensch. Proc. Ser. A = Indagationes Math.*, **19**(1957) 212–219; *MR* **19**, 252.
P. Erdős, On the irrationality of certain series, *Math. Student*, **36**(1968) 222–226 (1969); *MR* **41** #6787.
P. Erdős, Some problems and results on the irrationality of the sum of infinite series, *J. Math. Sci.*, **10**(1975) 1–7.
P. Erdős & E. G. Straus, On the irrationality of certain Ahmes series, *J. Indian Math. Soc.*, **27**(1963) 129–133 (1969); *MR* **41** #6787.

E25. Silverman 序列

序列

$$1,2,2,3,3,4,4,4,5,5,5,6,6,6,6,$$
$$7,7,7,7,8,8,8,8,9,9,9,9,9,\cdots$$

定义如下：$f(1)=1$，而 $f(n)$则是 n 在一个非减的整数序列中出现的次数，这个序列在本书第一版中归属于 David Silverman. Golomb 提出一个问题，这个问题由他、van Lint 以及 Marcus 和 Fine(见下面的文献)给出了解答：它的第 n 项的渐近表示的确是 $\tau^{2-\tau}n^{\tau-1}$，这里 τ 是黄金分割数$(1+\sqrt{5})/2$. 其误差项由 Ilan Vardi 作了研究，他猜想有

$$E(n)=\Omega_{\pm}\left(\frac{n^{\tau-1}}{\ln n}\right),$$

其中符号 $E(n)=\Omega_{\pm}(g(n))$的含意是：存在常数 c_1,c_2，使分别对无穷多个 n 有$E(n)>c_1g(n)$和 $E(n)<-c_2g(n)$成立，但是他甚至无法证明$|E(n)|$无界. 他还提出了一些没有解决的问题.

Marshall Hall 证明了：存在一个序列，使得每一个正整数可以惟一地表示成为该序列中两个元素的差. 例如由 $a_1=1,a_2=2$, $a_{2n+1}=2a_{2n}, a_{2n+2}=a_{2n+1}+r_n$ 所定义的序列

$$1,2,4,8,16,21,42,51,102,112,224,$$
$$235,470,486,972,990,1980,2001,\cdots,$$

其中 r_n 是不能表示成形式$a_j-a_i(1\leqslant i<j\leqslant 2n+1)$的最小自然

数. 还有其他可能的序列,但是求其中有最小渐近增长性的序列仍然是一个没有解决的问题.

参考文献

J. Browkin, Solution of a certain problem of A. Schinzel (Polish), *Prace Mat.*, **3**(1959) 205–207.

R. L. Graham, Problem E1910, *Amer. Math. Monthly*, **73**(1966) 775; remark by C. B. A. Peck, **75**(1968) 80–81.

M. Hall, Cyclic projective planes, *Duke Math. J.*, **4**(1947) 1079–1090.

Daniel Marcus & N. J. Fine, Solutions to Problem 5407, *Amer. Math. Monthly*, **74**(1967) 740–743.

Themistocles M. Rassias, A solution to a problem of R. K. Guy & D. Silverman in number theory, 84T-10-336, *Abstracts Amer. Math. Soc.*, **5**(1984) 330.

W. Sierpiński, *Elementary Theory of Numbers*, 2nd English edition (A. Schinzel) PWN, Warsaw, 1987, chap. 12,4 p. 444.

Ilan Vardi, The error term in Golomb's sequence, *J. Number Theory*, **40**(1992) 1–11; *MR* **93d**:11103.

E26. Epstein 的取放平方数游戏

Richard Epstein 的取放平方数游戏是用一堆豆子来玩的. 两个游戏者交替走着. 每走一着就是向其中加入或者从中减去该堆豆子中所含的最大的完全平方数. 即两人交替地指定非负整数 a_n,这里

$$a_{n+1} = a_n \pm \lfloor \sqrt{a_n} \rfloor^2,$$

首先取到零的人为胜. 这是一个很迷人的游戏,许多数都会导致平局. 例如从 2 出发,下一个游戏者不会取 1,因为那样会使他的对手获胜,于是他取 3. 现在加上 1 是一步坏着,于是他的对手又回到 2. 类似地,6 也导致平局,相应的最佳走法是:6,10,19!,35,60,109!,209!,13!,22!,6,…,其中的惊叹号(!)的含义是说这是一步好着,而不是表示阶乘(!)例如,在 209 后面取 405 是一步坏着,因为这样的话下一个人可以走到 5,而这是一个P-位置(P-position), 也就是上一个游戏者必胜的位置. 类似地,从 60 出发,取 11 是坏着,即是一个N-位置(N-position),也就是使下一个游戏者可能取胜的位置(下一个人走到 20 即可).

究竟是P-位置

0,5,20,29,45,80,101,116,135,145,165,173,236,257,397,404,445,477,540,565,580,629,666,836,845,885,909,944,949,954,975,1125,1177,⋯

还是N-位置

1,4,9,11,14,16,21,25,30,36,41,44,49,52,54,64,69,71,81,84,86,92,100,105,120,121,126,136,141,144,149,164,169,174,189,196,201,208,216,225,230,245,252,254,256,261,⋯

有正密度呢?

参考文献

E. R. Berlekamp, J. H. Conway & R. K. Guy, *Winning Ways for your Mathematical Plays*, Academic Press, London, 1982, Chapter 15.

E27. 最大和最小序列

Roger Eggleton 在他的硕士论文中讨论了最大序列(max sequence),它是从一个有限序列 $a_0, a_1, \cdots, a_n$,出发,用 $a_{n+1} = \max_i (a_i + a_{n-i})$来加以延拓定义所得到的无穷序列. 这方面的主要结果之一是:它的一阶差分最终是周期序列. 例如从 1,4,3,2 开始,我们得到 7,8,11,12,15,16,⋯,相应的差分是 3,−1,−1,5,1,3,1,3,1,⋯对**最小序列**(mex sequence)会发生什么呢? 这里一组非负整数的**最小**(mex)是指这个集合以外最小的数,也就是不出现在此集合中的最小的非负整数. 从序列 1,4,3,2 出发不断做出集合$\{a_i + a_{n-i}\}$的最小,例如(此段原书有误,在征求了原作者的意见后作了改写):

$$\text{mex}\{1+2, 4+3\} = 0,$$
$$\text{mex}\{1+0, 4+2, 3+3\} = 0,$$
$$\text{mex}\{1+0, 4+0, 3+2\} = 0,$$
$$\text{mex}\{1+0, 4+0, 3+0, 2+2\} = 0,$$

$$\text{mex}\{1+0,4+0,3+0,2+0\}=0,$$
$$\text{mex}\{1+0,4+0,3+0,2+0,0+0\}=5,$$
$$\text{mex}\{1+5,4+0,3+0,2+0,0+0\}=1,$$

如此继续下去得到

0,0,0,0,0,5,1,1,1,1,1,6,2,2,0,0,0,0,0,5,1,1,1,1,1,6,⋯.

这个序列最终是周期序列吗?

A. S. Fraenkel 注意到序列 $a_i=\lfloor i\alpha\rfloor$(其中 α 是任何实数),它满足不等式

$$\max(a_{n-i}+a_i)\leqslant a_n\leqslant 1+\min(a_{n-i}+a_i),$$
$$1\leqslant i<n,\quad n=2,3,\cdots.$$

例如 $\alpha=\frac{1}{2}(1+\sqrt{5})$生成序列 1,3,4,6,8,9,11,12,14,16,17,19,21,⋯,它和序列$\lfloor i\beta\rfloor$(这里 $1/\alpha+1/\beta=1$)相匹配. 这些 Beatty 序列(Beatty sequence)合起来就作成了 Wythoff 对(Wythoff pair).

这个问题的原动力来自用 Sprague-Grundy 理论对八进位游戏(octal game)的分析,其中通常的加法被匿门加法(nim addition),即以 2 为底且没有进位的加法,也就是异或(XOR)所代替. 现在 1,4,3,2 就导出序列

0,0,0,0,0,5,1,4,1,1,1,3,6,6,6,3,0,2,2,2,7,2,4,1,⋯.

这种序列的性状仍有相当神秘的色彩,把它们弄清楚将会得出有关类匿门博奕(nim-like game)的结果.

参 考 文 献

S. Beatty, Problem 3173, *Amer. Math. Monthly*, **33** (1926) 159 (and see J. Lambek & L. Moser, **61** (1954) 454.

E. R. Berlekamp, J. H. Conway & R. K. Guy, *Winning Ways for your Mathematical Plays*, Academic Press, London, 1982, Chapter 4.

Michael Boshernitzan & Aviezri S. Fraenkel, Nonhomogeneous spectra of numbers, *Discrete Math.*, **34**(1981) 325-327; *MR* **82d**: 10077.

Michael Boshernitzan & Aviezri S. Fraenkel, A linear algorithm for nonhomogeneous spectra of numbers, *J. Algorithms*, **5**(1984) 187-198; *MR* **85j**:11183.

R. B. Eggleton, Generalized integers, M.A. thesis, Univ. of Melbourne, 1969.

Ronald L. Graham, Lin Chio-Shih & Lin Shen, Spectra of numbers, *Math. Mag.*, **51**(1978) 174-176; *MR* **58** #10808.

E28. B_2-序列

我们称一个无穷序列 $1\leqslant a_1<a_2<\cdots$是一个 A-序列(A-sequence)，如果没有哪个 a_i 能是该序列中异于 a_i 的若干不同元素之和. Erdös 证明了:对每个 A-序列有 $\sum 1/a_i<103$，而 Levine 和 O'Sullivan 将它改进到 4. 他们还给出了一个 A-序列,它的元素的倒数之和 >2.035. Abbott,后来有张振祥(Zhang Zhen-Xiang)给出例子

$\{1,2,4,8,1+24k,35950+24t: 1\leqslant k\leqslant 55,1\leqslant t\leqslant 44\}$,

这将上述的上界改进为 2.0648. 进一步取一段序列的项能将此下界改进为 2.0649,但是未能达到 2.065.

如果 $1\leqslant a_1<a_2<\cdots$是一个 B_2-序列(与 C9 比较),即其所有数对之和皆不相同的序列, $\sum 1/a_i$ 的最大值是什么? 根据是否允许 $i=j$,相应有两个问题,但 Erdös 没法解决其中任何一个问题.

最显然的 B_2-序列是用贪婪算法得到的序列(与 E10 比较). 它的每一项是大于前面的项的最小整数,它不违反有不同的和这一条件,并且允许 $i=j$:

$$1,2,4,8,13,21,31,45,66,81,97,123,148,182,\cdots.$$

Mian 和 Chowla 用它证明了满足 $a_k\ll k^3$ 的 B_2-序列的存在性. 如果 M 是 $\sum 1/a_i$ 经过所有 B_2-序列时取到的最大值,而 S^*是 Mian-Chowla 序列的元素的倒数之和,那么 $M\geqslant S^*>2.156$. 但是 Levine 注意到如果 $t_n=n(n+1)/2$,那么就有 $M\leqslant\sum 1/(t_n+1)<2.374$，他问:是否有 $M=S^*$? 张振祥指出有 $S^*<2.1596$ 以及 $M>2.1597$,从而推翻了上述结论. 在 Mian-Chowla 序列中用 229 代替该序列的下面一项 204,然后继续用贪婪算法,就可以得到上面最后那个结果.

令 $a_1<a_2<\cdots$是一个无穷整数序列,其中所有的三数和 a_i+

$a_j + a_k$ 都不相同. Erdös 悬赏 500 美元给能对他的一个早期的猜想 $\lim a_n/n^3 = \infty$ 给出证明或者推翻此猜想的人.

参考文献

H. L. Abbott, On sum-free sequences, *Acta Arith.*, **48**(1987) 93–96.

P. Erdős, Problems and results in combinatorial analysis and combinatorial number theory, *Graph Theory, Combinatorics and Applications*, Vol. 1 (Kalamazoo MI, 1988) 397–406, Wiley, New York, 1991.

Eugene Levine, An extremal result for sum-free sequences, *J. Number Theory*, **12**(1980) 251–257.

Eugene Levine & Joseph O'Sullivan, An upper estimate for the reciprocal sum of a sum-free sequence, *Acta Arith.*, **34**(1977) 9–24; *MR* **57** #5900.

Abdul Majid Mian & S. D. Chowla, On the B_2-sequences of Sidon, *Proc. Nat. Acad. Sci. India Sect. A*, **14**(1944) 3–4; *MR* **7**, 243.

J. O'Sullivan, On reciprocal sums of sum-free sequences, PhD thesis, Adelphi University, 1973.

Zhang Zhen-Xiang, A sum-free sequence with larger reciprocal sum, *Discrete Math.*, (1992)

Zhang Zhen-Xiang, A B_2-sequence with larger reciprocal sum, *Math. Comput.*, **60**(1993) 835–839.

Zhang Zhen-Xiang, Finding finite B_2-sequences with larger $m - a_m^{1/2}$, *Math. Comput.*, **61**(1993); *MR* **93m**:11012.

E29. 所有的和与积都在该序列分成的两个类之一的序列

把整数分化成两个类. 是否总有一个序列 $\{a_i\}$,使得所有的和 $\sum \varepsilon_i a_i$ 和所有的乘积 $\prod a_i^{\varepsilon_i}$ (其中 ε_i 是 0 或 1,且和与乘积中各只有有限多个数不是 0)都在同一个类中呢? Hindman 对 Erdös 的这个问题给出了否定的回答.

是否存在一个序列 $a_1 < a_2 < \cdots$,使所有的和 $a_i + a_j$ 与所有的乘积 $a_i a_j$ 都在同一个类中呢? Graham 证明了:如果我们把整数 [1,252]分化成两个类,则有 4 个不同的数 $x, y, x+y$ 和 xy 全都在同一个类中. 此外,252 还是最好可能的了. Hindman 证明了:如果把整数[2,990]分划成两个类,那么有一个类必包含 4 个不同的数 $x, y, x+y$ 和 xy. 对≥3 的整数没有对应的结果.

Hindman 还证明了：如果我们把整数分化成两个类，则总存在一个无穷序列$\{a_i\}$，使所有的和 a_i+a_j（允许取 $i=j$）都在同一个类中．另一方面，他找到了分化成 3 个类的一种分解法，其中不存在这样的无穷序列．

参考文献

J. Baumgartner, A short proof of Hindman's theorem, *J. Combin. Theory Ser. A*, **17**(1974) 384–386.

Neil Hindman, Finite sums with sequences within cells of a partition of *n*, *J. Combin. Theory Ser. A*, **17**(1974) 1–11.

Neil Hindman, Partitions and sums and products of integers, *Trans. Amer. Math. Soc.*, **247**(1979) 227–245; *MR* **80b**:10022.

Neil Hindman, Partitions and sums and products — two counterexamples, *J. Combin. Theory Ser. A*, **29**(1980) 113–120.

E30．MacMahon 的度量素数

MacMahon 的“度量素数”

$$1,2,4,5,8,10,14,15,16,21,22,25,$$
$$26,28,33,34,35,36,38,40,42,\cdots$$

是通过将序列中前面所有的两个或多个相连的元素之和剔除以后而生成的．

如果 m_n 是该序列中第 n 个数，M_n 是前 n 个元素之和，则 George Andrew 猜想

$$¿\quad m_n \sim n(\ln n)/\ln\ln n \quad ?$$

和

$$¿\quad M_n \sim n^2(\ln n)/\ln(\ln n)^2 \quad ?$$

他还提出了下述的可能更容易一些的问题：证明对某个 $\Delta<2$ 有 $\lim n^{-\Delta}m_n=0$；证明有 $\lim m_n/n=\infty$；证明对每个 n 有 $m_n<p_n$，这里 p_n 是第 n 个素数．

Jeff Lagarias 建议只剔除前面两个或 3 个相邻的项的和，他问：产生的序列

1,2,4,5,8,10,12,14,15,16,19,20,21,24,25,27,28,32,33,

34,37,38,40,42,43,44,46,47,48,51,53,54,56,57,58,59,
61,...

的密度是否为$\frac{3}{5}$? Don Coppersmith 有一个更有说服力的推理,它倾向于否定的答案.

更为一般地,如果 $1\leqslant a_1<a_2<\cdots<a_k\leqslant n$ 是一个序列,其中没有一个元素 a 能是该序列中前面若干个相连的元素之和,那么 Pomerance 发现 $\max k\geqslant\left\lfloor\frac{n+3}{2}\right\rfloor$,其后 Róbert Freud 证明了 $\max k\geqslant\frac{19}{36}n$. 他们与 Erdös 注意到:即使仅仅不允许每个元素是它前面某两个连续项的和,也会有 $\max k\leqslant\frac{2}{3}n$. Coppersmith 和 Phillips 已经证明了 $\max\geqslant\frac{13}{24}n-O(1)$,并将上界降低到

$$\max k\leqslant\left(\frac{2}{3}-\varepsilon\right)n+O(\ln n),\quad 其中\ \varepsilon=\frac{1}{896}.$$

Erdös 问:该序列的下密度是否为 0? 看来似乎有

$$¿\quad \frac{1}{\ln x}\sum_{a_i<x}\frac{1}{a_i}\to 0 \qquad ?$$

参考文献

G. E. Andrews, MacMahon's prime numbers of measurement, *Amer. Math. Monthly*, **82**(1975) 922–923.

Don Coppersmith & Steven Phillips, On a question of Erdős on subsequence sums, (preprint, Nov. 1992).

Róbert Freud, *James Cook Math. Notes*, Jan. 1993.

R. L. Graham, Problem 1910, *Amer. Math. Monthly*, **73**(1966) 775; solution **75**(1968) 80–81.

Jeff Lagarias, Problem 17, W. Coast Number Theory Conf., Asilomar, 1975.

P. A. MacMahon, The prime numbers of measurement on a scale, *Proc. Cambridge Philos. Soc.*, **21**(1923) 651–654.

Štefan Porubský, On MacMahon's segmented numbers and related sequences, *Nieuw Arch. Wisk.*(3) **25**(1977) 403–408; *MR* **58** #5575.

N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, New York, 1973; sequences 363, 416, 1044.

E31. Hofstadter 的 3 个序列

Douglas Hofstadter 定义了 3 个令人感兴趣的序列.

(a) $a_1=a_2=1$,对 $n\geqslant 3$ 有 $a_n=a_{n-a_{n-1}}+a_{n-a_{n-2}}$. 这个序列的一般性状如何?

1,1,2,3,3,4,5,5,6,6,6,8,8,8,10,9,10,11,11,

12,12,12,12,16,14,14,16,16,16,16,20,17,17,…

有无穷多个整数 7,13,15,18,…不在这个序列中吗?

(b) $b_1=1,b_2=2$,对 $n\geqslant 3$, b_n 是大于 b_{n-1} 且能表为该序列中两个或多个相连的项之和的最小整数,从而有

1,2,3,5,6,8,10,11,14,16,17,18,19,21,22,24,25,29,

30,32,33,34,35,37,40,41,43,45,46,47,49,51,…

这是 MacMahon 的度量素数的一种对偶(E30). 此序列是如何增长的呢?

(c) $c_1=2,c_2=3$,又当 $c_1,\cdots,c_n$ 定义好以后,作出所有可能的表达式

$c_ic_j-1\ (1\leqslant i<j\leqslant n)$,并将它们补充到序列中:

2,3,5,9,14,17,26,27,33,41,44,50,51,53,65,69,77,

80,81,84,87,98,99,101,105,122,125,129,…

这个结果包含几乎所有的整数吗?

Conway 给出过一个与这 3 个序列中的第一个类似的序列:

1,1,2,2,3,4,4,4,5,6,7,7,8,8,8,8,9,…,

对 $n\geqslant 3$,它定义为

$$a(n)=a(a(n-1))+a(n-a(n-1)).$$

一些困难的问题已经在 Mallows 的一篇引人入胜的论文中给出了解答. Zeitlin 得到了一些恒等式. Conway 的序列的一个变形是定义

$$b(n)=b(b(n-1))+b(n-1-b(n-1)),$$

不过这涉及到上面那个由 $b(n-1)=n-a(n)$ 定义的序列. 但是

如果我们记

$$c(n) = c(c(n-2)) + c(n-c(n-2)),$$

那么其增长就变得很不规则了,我们甚至不清楚 $c(n)/n$ 是否有极限.

参 考 文 献

W. A. Beyer, R. G. Schrandt & S. M. Ulam, Computer studies of some history-dependent random processes, LA-4246, Los Alamos Nat. Lab., 1969.

J. H. Conway, Some crazy sequences, videotaped talk at A.T. & T. Bell Laboratories, 88-07-15.

Peter J. Downey & Ralph E. Griswold, On a family of nested recurrences, *Fibonacci Quart.*, 22(1984) 310–317; *MR* **86e**:11013.

P. Erdős & R. L. Graham, Old and New Problems and Results in Combinatorial Number Theory, *Monographie de L'Enseignement Mathématique, Genève*, **28**(1980) 83–84.

Douglas R. Hofstadter, *Gödel, Escher, Bach*, Vintage Books, New York, 1980, p. 137.

Mark Kac, A history-dependent random sequence defined by Ulam, *Adv. in Appl. Math.*, **10**(1989) 270–277; *MR* **91c**:11042.

Péter Kiss & Béla Zay, On a generalization of a recursive sequence, *Fibonacci Quart.*, **30**(1992) 103–109; *MR* **90e**:11022.

Colin L. Mallows, Conway's challenge sequence, *Amer. Math. Monthly*, **98** (1991) 5–20.

David Newman, Problem E3274, *Amer. Math. Monthly*, **95**(1988) 555.

Stephen M. Tanny, A well-behaved cousin of the Hofstadter sequence, *Discrete Math.*, **105**(1992) 227–239; *MR* **93i**:11029.

David Zeitlin, Explicit solutions and identities for Conway's iterated sequence, *Abstracts Amer. Math. Soc.*, **12**(1991).

E32. 由贪婪算法形成的 B_2 序列

Dickson 的一个老问题仍未获得解决. 给定一组 k 个整数 $a_1 < a_2 < \cdots < a_k$, 对 $n \geqslant k$, 定义 a_{n+1} 是大于 a_n 且不是形如 $a_i + a_j$ $(i, j \leqslant n)$ 的最小整数. 除了在序列开头预先指定的一段元素外, 这些数是由贪婪算法得出的无和序列(与 C9, C14, E10 以及 E28 比较).

由差 $a_{n+1} - a_n$ 组成的序列最终会成为周期序列吗?

这样的序列在出现周期性之前可能要经过很长时间. 例如,

即便对 $k=2$,如果我们取 $a_1=1, a_2=6$,序列即为

$$1,6,8,10,13,15,17,22,24,29,31,33,36,$$
$$38,40,45,47,52,54,56,59,61,63,68,\cdots,$$

如果有人没有立即辨认出它的类型,这是可以原谅的. 试从集合 $\{1,4,9,16,25\}$ 出发,在经过 82 个不规则的差之后,它才有长为 224 的周期.

Queneau(见 C4 的参考文献)考虑了用 $i<j\leqslant n$ 代替 $i,j\leqslant n$ 而得到的类似的问题. 猜想这样的 0-加性序列(0-additive sequence)最终会变成有周期性的差. Steven Finch 计算了该序列的 1500000 项,它的头 6 个项由 $\{3,4,6,9,10,17\}$ 给出,他没有发现其差序列最终会变成周期序列的任何迹象.

Selmer 告诉我说, Dickson 的问题是 Stöhr 序列(Stöhr sequence)当 $h=2$ 时的特例:令 $a_1=1$,对 $n\geqslant k$ 定义 a_{n+1} 是大于 a_n 且不能表为 $a_1, a_2, \cdots, a_n$ 中至多 h 个加数之和的最小整数. 与 C12 中的 h-基比较. 在绝大多数情形,差 $a_{n+1}-a_n$ 组成的序列最终都成为周期序列,但也有一些情形,其差组成的序列并未发现有周期性.

参考文献

Neil J. Calkin, Sum-free sets and measure spaces, PhD thesis, Univ. of Waterloo, 1988.

Neil J. Calkin & Steven R. Finch, Necessary and sufficient conditions for a sum-free set to be ultimately periodic (preprint, 1993).

Peter J. Cameron, Portrait of a typical sum-free set, Surveys in Combinatorics 1987, *London Math. Soc. Lecture Notes*, **123**(1987) Cambridge Univ. Press, 13–42.

L. E. Dickson, The converse of Waring's problem, *Bull. Amer. Math. Soc.*, **40** (1934) 711–714.

Steven R. Finch, Are 0-additive sequences always regular? *Amer. Math. Monthly*, **99**(1992) 671–673.

Ernst S. Selmer, On Stöhr's recurrent h-bases for N, *Kgl. Norske Vid. Selsk. Skrifter*, **3**(1986) 1–15.

Ernst S. Selmer & Svein Mossige, Stöhr sequences in the postage stamp problem, No. **32**(Dec. 1984) Dept. Pure Math., Univ. Bergen, ISSN 0332-5407.

E33. 不包含单调算术级数的序列

Erdös 和 Graham 称一个序列 $\{a_i\}$ 有一个长为 k 的**单调的**(monotone)算术级数, 如果存在下标 $i_1 < i_2 < \cdots < i_k$, 使得子列 $a_{i_j}(1 \leqslant j \leqslant k)$或者是一个递增的算术级数,或者是一个递减的算术级数. 如果 $M(n)$是$[1, n]$的没有 3 项单调算术级数的排列的个数,则 Davis 和其他人证明了

$$M(n) \geqslant 2^{n-1}, \quad M(2n-1) \leqslant (n!)^2,$$
$$M(2n) \leqslant (n+1)(n!)^2.$$

他们问:$M(n)^{1/n}$是否有界?

Davis 和其他人还证明了:(所有)正整数的任何排列都必定包含一个递增的 3 项算术级数,然而有这样的排列存在,它没有单调的 5 项算术级数. 还不知道是否总有单调的 4 项算术级数出现.

如果正整数被表示为一个双无穷的序列,那么必定仍然会出现一个单调的 3 项算术级数,但是 4 项的算术级数有可能不出现.

如果所有整数都被排列起来,则 Tom Odda 证明了:在排列成单无穷的情形,不一定有 7 项的算术级数出现,但是除此而外所知甚少.

参 考 文 献

J. A. Davis, R. C. Entringer, R. L. Graham & G. J. Simmons, On permutations containing no long arithmetic progressions, *Acta Arith.*, **34**(1977) 81-90; *MR* **58** #10705.

Tom Odda, Solution to Problem E2440, *Amer. Math. Monthly*, **82**(1975) 74.

E34. 幸 福 数

Reg Allenby 的女儿就读于英国的学校,回家时她把**幸福数**(happy number)这一概念带了回来. 如果你重复对一个数的十进位数字求平方和这一程序,则易见要么你得到圈

$$4 \to 16 \to 37 \to 58 \to 89 \to 145 \to 42 \to 20 \to 4,$$

要么你得到 1. 在后一情形,你是从一个幸福数开始的. 前一百个幸福数是

1	7	10	13	19	23	28	31	32	44	49	68	70	79	82	86	91	94	97	100
103	109	129	130	133	139	167	176	188	190	192	193	203	208	219	226	230	236	239	262
263	280	291	293	301	302	310	313	319	320	326	329	331	338	356	362	365	367	368	376
379	383	386	391	392	397	404	409	440	446	464	469	478	487	490	496	536	556	563	565
566	608	617	622	623	632	635	637	638	644	649	653	655	656	665	671	673	680	683	694

看起来所有的数中大约有 1/7 的数是幸福数,但是对这种数的密度的界,可以证明什么呢? 可以得到多少个连续的幸福数呢? 可以有任意多个连续的幸福数吗? 第一对连续幸福数是 31,32;第一组连续的 3 个幸福数是 1880,1881,1882,一组连续的 5 个幸福数的例子是 44488,44489,44490,44491,44492. 请用所给幸福数组中元素的大小给出这种连续的幸福数的个数的界. 幸福数组成的序列中相邻两数间的间隙能有多大? 我们可以定义一个幸福数的**高度**(height)是到达 1 所需做的迭代的次数. 例如高度最小的几个幸福数是:

高度	0	1	2	3	4	5	6
数	1	10	13	23	19	7	356.

78999 是高度为 7 的最小的幸福数吗? 请给出高度为 h 的最小的幸福数的大小的界.

如果用立方代替平方,那么至少基数为 10 的情形是我们所掌握的,这是根据如下事实:完全立方数必同余于 0 或 $\pm 1 \bmod 9$. 对应的数(1,10,100,112,121,211,778,…)的密度可以是0. 模 3 余 0 的数收敛于 153,模 3 余 2 的数收敛于 371 或 407,故而只限于关注模 3 余 1 的数即可. 这样的数或者收敛于 370,或者收敛于 3-圈(55,250,133)或(160,217,352)中的一个数,或者收敛于 2-圈(919,1459)或(136,244)中的一个数,或者偶而也恰好收敛于 1. 上述每一情形各占多大比例?

对更高次的幂结论如何呢? 对于不同的基数结论又如何?

参考文献

Henry Ernest Dudeney, *536 Puzzles & Curious Problems* (edited Martin Gardner), Scribner's, New York, 1967, Problem 143, pp. 43, 258–259.

Joseph S. Madachy, *Mathematics on Vacation*, Scribner's, New York, 1966, pp. 163–165.

E35. Kimberling 洗牌

Clark Kimberling 考虑了数的阵列：

[1]	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	[3]	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
4	2	[5]	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
6	2	7	[4]	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
8	7	9	2	[10]	6	11	12	13	14	15	16	17	18	19	20	21	22	23
6	2	11	9	12	[7]	13	8	14	15	16	17	18	19	20	21	22	23	24
13	12	8	9	14	11	[15]	2	16	6	17	18	19	20	21	22	23	24	25
2	11	16	14	6	9	17	[8]	18	12	19	13	20	21	22	23	24	25	26
18	17	12	9	19	6	13	14	[20]	16	21	11	22	2	23	24	25	26	27
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

表中每一行是在上一行用方框标出(并去掉)位于主对角线上的那个元素，然后记下这个方框后面的第一个数，再记下这个方框前面的第一个数，再记下这个方框后面的第二个数，再记下这个方框前面的第二个数，如此下去，直到把原来所有的数都写完为止，然后再继续对所有剩下的数(仍然按照数字的大小顺序). 是否最后每一个数都会被去掉呢?

诸数	1	2	3	4	5	6	7	8	9	10
在下面各行被去掉	1	25	2	4	3	22	6	8	10	5
诸数	11	12	13	14	15	16	17	18	19	20
在下面各行被去掉	32	83	44	14	7	66	169	11	49595	9

诸数	40	68	106	147
在下面各行被去掉	93167	181393	270186	8765242
诸数	242	322	502	669
在下面各行被去掉	16509502	38293016	118850522	653494691

按照另一种从方框的右边和左边的记数法,我们可以改为先从方框左边第一个数开始,这样得到阵列

[1]	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
2	[3]	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	4	[5]	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
4	6	2	[7]	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	8	6	9	[4]	10	11	12	13	14	15	16	17	18	19	20	21	22	23
9	10	6	11	8	[12]	2	13	14	15	16	17	18	19	20	21	22	23	24
8	2	11	13	6	14	[10]	15	9	16	17	18	19	20	21	22	23	24	25
14	15	6	9	13	16	11	[17]	2	18	8	19	20	21	22	23	24	25	26
11	2	16	18	13	8	9	19	[6]	20	15	21	14	22	23	24	25	26	27
……																		

它展示出一种类似的无序性状.

在每一个数的阵列中都有少量的图案:观察马沿公差为 3 的算术级数的移动. 例如,在原来的阵列中,对每个 $y \geqslant 0$,数 $n+3y$ 在第 $x+y$ 行的位置 $2y+1$ 上,其中对每个 $t \geqslant 0$,分别当

$$x = 3 \cdot 2^t - 1, \quad 4 \cdot 2^t - 1, \quad 5 \cdot 2^t - 1$$

时有

$$n = 9 \cdot 2^t - 3t - 7, \quad n = 12 \cdot 2^t - 3t - 8,$$
$$n = 15 \cdot 2^t - 3t - 9.$$

因此在第 $2x-1=2y+1$ 行,数 $n+3y$ 被去掉. 也即对 $t=-1, 0, 1, \cdots$,分别在第$6 \cdot 2^t - 3$行、第 $8 \cdot 2^t - 3$ 行以及第 $10 \cdot 2^t - 3$ 行,数 $n = 18 \cdot 2^t - 3t - 13, 24 \cdot 2^t - 3t - 14$ 以及 $30 \cdot 2^t - 3t - 15$ 相继被去掉.

参 考 文 献

Clark Kimberling, Problem 1615, *Crux Mathematicorum*, **17**#2(Feb 1991) 44.

E36. Klarner-Rado 序列

序列

1,2,4,5,8,9,10,14,15,16,17 ,18,20,26,27,28,29,30,32, 33,34,36,40,44,47,50,51,52,53,54,56,57,58,60,62,63,64, 66,68,72,80,83,86,87,88,89,92,93,94,98,99,100,101,102, 104,105,106,108,110,111,112,114,116,120,122,123,124,126, 128,132,134,136,⋯

是包含 1 且只要它包含 x,就必也包含 $2x$,$3x+2$ 和 $6x+3$ 的最薄的序列. 这个序列有正密度吗?

在论文

David A. Klarner & Richard Rado, Arithmetic properties of certain recursively defined sets, *Pacific J. Math.*, **53** (1974) 445-463.

中也问到几个这种类型的问题. 在数学评论(*MR* 50 ♯9784)上说到:其后的一篇论文(论文题目是"Sets generated by a linear operation", 同一杂志,待发表)解决了这篇论文中的许多猜想. 那篇论文发表了吗? 也请参看以下的文献.

参 考 文 献

David A. Klarner & Richard Rado, Linear combinations of sets of consecutive integers, *Amer. Math. Monthly*, **80**(1973) 985–989.

David A. Klarner & Karel Post, Some fascinating integer sequences, *Discrete Math.*, **106/107**(1992) 303–309; *MR* **93i**:11031.

E37. 老鼠陷阱

Cayley 引进了他称之为**老鼠陷阱**(mousetrap)的一个排列问题,它大致以扑克牌游戏 Treize 为基础. 假设将诸数 $1,2,\cdots,n$ 写在牌上,每张牌上写一个数. 经过洗牌(排列)之后,开始从上向下给这副牌点数. 如果牌上的数不等于点的数,就把这张牌放到最后去,再继续点数. 如果某张牌的两个数相等,就把这张牌拿掉,并再从 1 开始点数. 如果所有的牌都被拿掉了,你就赢了;但是如果点数点到 $n+1$,你就输了. Cayley 提出两个问题:

1. 对每个 n,求出 $1,2,\cdots,n$ 的所有能取胜的排列.

2. 对每个 n,求出对每个 $i(1\leqslant i\leqslant n)$恰好能去掉 i 张牌的那种排列的个数.

第三个问题是在我们的研究中提出来的. 考虑一个把每个数都能去掉的排列. 把这些数按照它们被去掉的顺序所作成的一列数又是一个排列. 用这种方法得到的这又一个排列称为**重新编队**(reformed)排列.

3. 刻画重新编队排列的特征.

排列 4213 是一个取胜排列,它给出排列 2134;接下去它又给出重新编队排列 3214,这不再是一个取胜的排列.

4. 对给定的 n,重新编队排列的最长的序列是什么?

5. 有任意长的序列吗? 除了

$$1\rightarrow1\rightarrow1\rightarrow1\cdots \quad 和 \quad 12\rightarrow12\rightarrow12\rightarrow12\cdots$$

以外,还有别的圈吗?

模老鼠陷阱(modular mousetrap). 我们可以改为对 $n,n+1,\cdots$点数来玩老鼠陷阱游戏,我们可以再从$\cdots,n,1,2,\cdots$开始,现在至少有许多牌被去掉了. 事实上,如果 n 是一个素数,那么或者原来的牌是一个重排,或者所有的牌都被去掉了,因此每个序列都成了圈,或者终止于一个重排. 恒等排列 $123\cdots n$ 总是做成一个 1-圈,现在也有非平凡的圈的例子了.

6. 对每个 k 都有k-圈吗？产生出一个 k-圈的最小的 n 是多少？

参考文献

A. Cayley, A Problem in Permutations, *Quart. Math. J.*, **I**(1857), 79.

A. Cayley, On the Game of Mousetrap, *Quart. J. Pure Appl. Math.*, **XV** (1877), 8-10.

A. Cayley, A Problem on Arrangements, *Proc. Roy. Soc. Edinburgh*, **9**(1878) 338–342.

A. Cayley, Note on Mr. Muir's Solution of a Problem of Arrangement, *Proc. Roy. Soc. Edinburgh*, **9**(1878) 388–391.

Richard K. Guy & Richard J. Nowakowski, Mousetrap, Proc. Erdős80 Keszthely Combin. Conf., 1993. [see also *Amer. Math. Monthly*, **101**(1994).]

T. Muir, On Professor Tait's Problem of Arrangement, *Proc. Royal Soc. Edinburgh*, **9**(1878) 382–387.

T. Muir, Additional Note on a Problem of Arrangement, *Proc. Royal Soc. Edinburgh*, **11**(1882) 187–190.

Adolf Steen, Some Formulae Respecting the Game of Mousetrap, *Quart. J. Pure Appl. Math.*, **XV**(1878), 230-241.

Peter Guthrie Tait, *Scientific Papers*, vol. 1, Cambridge, 1898, 287.

E38. 奇 序 列

称一个由 n 个 0 和 1 组成的序列$\{a_1,\cdots,a_n\}$是**奇的**(odd)，如果 n 个和 $\sum_{i=1}^{n-k} a_i a_{i+k}$ 中的每一个都是奇数($k=0,1,\cdots,n-1$). 例如，1101 是奇序列. Pelikán 猜想：如果 $n\geqslant5$，则没有奇数列. 但是 Peter Alles 证明了有无穷多个奇数列：如果 o 是一个长为 n 的奇序列，x 和 z 分别是有 $n-1$ 个 0 以及有 $3n-2$ 个 0 的序列，那么 oxozo 和 ozoxo 都是长为 $7n-3$ 的奇序列. 对于

$n=$	1	4	12	16	24	25	36	37	40	45
他找到	1	2	2	8	2	4	2	16	2	16

个奇序列，而且在 $n\leqslant50$ 以内不再有其他的奇序列了. 例如，101011100011 以及它的倒序所得的序列皆是奇序列. 他问：(奇序列的)长度 n 是否总是模 4 余 0 或余 1 的？当存在奇序列时，它的个数是否总是 2 的幂？

参考文献

Peter Alles, On a conjecture of J. Pelikán, *J. Combin. Theory Ser. A*, **60** (1992) 312–313; *MR* **93i**:11028.

J. Pelikán, Problem, in *Infinite and Finite Sets, Vol. III* (*Keszthely*, 1973), 1549, *Colloq. Math. Soc. János Bolyai*, **10**, North-Holland, Amsterdam, 1975.

F. 不在上述各章中的其他问题

在由若干杂题组成的这一章中，头几个问题是关于**格点**(lattice point)的．所谓格点即有整数坐标的点，它们大多是二维的问题，但有一些也可以表为高维的形式．下面是一些有趣的书．

参 考 文 献

J. W. S. Cassels, *Introduction to the Geometry of Numbers*, Springer-Verlag, New York, 1972.

L. Fejes Tóth, *Lagerungen in der Ebene, auf der Kugel und in Raum*, Springer-Verlag, Berlin, 1953.

J. Hammer, *Unsolved Problems Concerning Lattice Points*, Pitman, 1977.

O.-H. Keller, *Geometrie der Zahlen*, Enzyklopedia der Math. Wissenschaften **12**, B. G. Teubner, Leipzig, 1954.

C. G. Lekkerkerker, *Geometry of Numbers*, Bibliotheca Mathematica **8**, Walters-Noordhoff, Groningen; North-Holland, Amsterdam, 1969.

C. A. Rogers, *Packing and Covering*, Cambridge Univ. Press, 1964.

F1. Gauss 格点问题

一个非常困难的未解决的问题是 **Gauss 问题**(Gauss problem)：中心在原点、半径为 r 的圆的内部有多少个格点？如果答案是 $\pi r^2+h(r)$，那么 Hardy 和 Landau 证明了 $h(r)$不能是 $o(r^{1/2}(\ln r)^{1/4})$．人们猜想有 $h(r)=O(r^{1/2+\varepsilon})$．Iwaniec 和 Mozzochi 证明了 $h(r)=O(r^{7/11+\varepsilon})$，而最好已知的结果是 Huxley 得到的 $h(r)=O(r^{46/73+\varepsilon})$．

在三维空间里我们可以对球和正四面体提出类似的问题．对 F22 中的直四面体，请看 Lehmer 的论文，也见许以敬(XuYijing)和丘成栋(Stephen Yau S. -T.)的论文，但是他们对 Overhangen 有关任意凸体的上界所给出的反例是不正确的．

参考文献

Chen Jing-Run, The lattice points in a circle, *Sci. Sinica*, **12**(1963) 633–649; *MR* **27** #4799.

Javier Cilleruello, The distribution of the lattice points on circles, *J. Number Theory*, **43**(1993) 198–202.

Andrew Granville, The lattice points of an n-dimensional tetrahedron, *Aequationes Math.*, **41**(1991) 234–241; *MR* **92b**:11070.

Martin Huxley, *Proc. London Math. Soc.* (to appear).

Aleksandar Ivić, Large values of the error term in divisor problems and the mean square of the zeta-function, *Invent. Math.*, **71**(1983) 513–520; *MR* **84i**:10046.

H. Iwaniec & C. J. Mozzochi, On the divisor and circle problems, *J. Number Theory*, **29**(1988) 60–93; *MR* **89g**:11091.

D. H. Lehmer, The lattice points of an n-dimensional tetrahedron, *Duke Math. J.*, **7**(1940) 341–353.

T. Overhagen, Zur Gitterpunktanzahl konvexer Körper im 3-dimensionalen euklidischen Raum, *Math. Ann.*, **216**(1975) 217–224; *MR* **57** #281.

Xu Yijing & Stephen Yau S.-T., A sharp estimate of the number of integral points in a tetrahedron, *J. reine angew. Math.*, **423**(1992) 199–219; *MR* **93d**:11067.

F2. 有不同距离的格点

能选取到使得$\binom{k}{2}$个相互距离全不相同的格点(x,y)，$1\leqslant x$，$y\leqslant n$，的最大个数 k 是什么？容易看出有 $k\leqslant n$. 对 $n\leqslant 7$ 这个界可以达到. 例如对 $n=7$ 有点(1,1)，(1,2)，(2,3)，(3,7)，(4,1)，(6,6)和(7,7)，但这并非对任意大的 n 的值都对. Erdös 和 Guy 证明了

$$n^{2/3-\varepsilon}<k<cn/(\ln n)^{1/4},$$

且他们猜想

$$¿\quad k<cn^{2/3}(\ln n)^{1/6}\quad ?$$

人们还可以求"浸润的(saturated)"构形，它包含个数最少的能确定不同距离的点，但是只要再加入一个格点就会使其中某一个距离重复出现. Erdös 注意到这至少需要 $n^{2/3-\varepsilon}$ 个格点. 在一维的情形，他未能对 $O(n^{1/3})$ 作出改进，并怀疑$O(n^{1/2+\varepsilon})$是否是最好可能的结果.

参考文献

P. Erdős & R. K. Guy, Distinct distances between lattice points, *Elem. Math.*, **25**(1970) 121–123; *MR* **43** #7406.

F3. 无四点共圆的格点

Erdös 和 Purdy 问：可以从 n^2 个格点 (x, y)，$1 \leqslant x, y \leqslant n$ 中选取多少个格点，使得其中没有四点共圆？易证可以选到 $n^{2/3-\epsilon}$ 个，但是有可能会得到更多这样的点.

使得我们可以从中选取 t 个格点，这些点决定的 $\binom{t}{2}$ 条直线能包含所有这 n^2 个格点的最小的 t 是什么？不难证明 $t > cn^{2/3}$，而 Noga Alon 则对任意维数 d 的问题得到界

$$cn^{d(d-1)/(2d-1)} \leqslant t(n, d) \leqslant Cn^{d(d-1)/(2d-1)} \ln n.$$

参考文献

Noga Alon, Economical coverings of sets of lattice points, *Geom. Funct. Anal*, **1**(1991) 224–230; *MR* **92g**:52017.

F4. 任意三点皆不共线的格点问题

$2n$ 个格点 (x, y) $(1 \leqslant x, y \leqslant n)$ 可否选取得使之没有任何三点共线？对 $2 \leqslant n \leqslant 32$ 以及对若干个大偶数 n，这已经做到了. Guy 和 Kelly 给出四个猜想：

1. 不存在具有矩形对称而没有完全的正方形对称的构形.

2. 仅有的具有完全的正方形对称的构形是图 17 中所示的构形. $n = 10$ 的构形首先由 Acland-Hood 得到. 对 $n \leqslant 60$，这一猜想已由 Flammenkamp 作了验证.

3. 对足够大的 n，开始所提问题的答案是“不”，也即该问题仅有有限多个解. 相应构形的总数(不计反射和旋转)是：

n	2	3	4	5	6	7	8	9	10	11	12	1
#	1	1	4	5	11	22	57	51	156	158	566	499

对于大的 n 的值,人们已对具有特殊对称的构形进行了计数.

图 17　$2n$ 个格点,无三点共线,$n=2,4,10$.

4. 对大的 n,我们可以选取至多$(c+\varepsilon)n$ 个格点,使无三点共线,其中 $3c^3=2\pi^2$,也即 $c\approx1.85$.

在相反的方向上,Erdös 证明了:如果 n 是素数,则能够选取 n 个点,使无三点共线,而 Hall, Jackson, Sudbery 和 Wild 证明了:对大的 n,可以找到$\left(\frac{3}{2}-\varepsilon\right)n$ 个这样的点.

T. Thiele 修改了 Erdös 的结构,从而证明了:可以找到$\left(\frac{1}{4}-\varepsilon\right)n$ 个无三点共线、无四点共圆的点.

无三点共线问题是 Heibronn 的一个老问题的离散类似. 把 $n(\geqslant 3)$个点放在一个单位面积的圆盘(或正方形,或等边三角形)中,使每三个点形成的三角形的最小面积取到最大值. 如果用 $\Delta(n)$记该最大面积,则 Heibronn 原来猜想有 $\Delta(n)<c/n^2$,但是 Komlós, Pintz 和 Szemerédi 通过证明 $\Delta(n)>(\ln n)/n^2$ 而推翻了这一猜想. Roth 证明了有 $\Delta(n)\ll 1/n(\ln\ln n)^{1/2}$;Schmidt 将它改进为 $\Delta(n)\ll 1/n(\ln n)^{1/2}$;而 Roth 后来又进一步改进为 $\Delta(n)$

$\ll 1/n^{\mu-\varepsilon}$,这里起初他得到 $\mu=2-2/\sqrt{5}>1.1055$,后来得到 $\mu=(17-\sqrt{65})/8>1.1172$.

在单位正方形中给定 $3n$ 个点($n\geqslant 2$),它们以很多种方式决定 n 个三角形. 选定一种分划,使面积之和最小,用 $a^*(n)$ 记这个最小和的最大值(最大值取过 $3n$ 个点的所有构形). 那么 Odlyzko 和 Stolarsky 证明了 $n^{-1/2}\ll a^*(n)\ll n^{-1/24}$. 如果要求那 n 个三角形面积不相交,我们甚至还不知道它们的面积之和是否趋向于 0.

参考文献

Acland-Hood, *Bull. Malayan Math. Soc.*, **0**(1952-53) E11–12.

Michael A. Adena, Derek A. Holton & Patrick A. Kelly, Some thoughts on the no-three-in-line problem, Proc. 2nd Austral. Conf. Combin. Math., *Springer Lecture Notes*, **403**(1974) 6–17; *MR* **50** #1890.

David Brent Anderson, Update on the no-three-in-line problem, *J. Combin. Theory Ser. A*, **27**(1979) 365–366.

W. W. Rouse Ball & H. S. M. Coxeter, *Mathematical Recreations & Essays*, 12th edition, University of Toronto, 1974, p. 189.

C. E. Corzatt, Some extremal problems of number theory and geometry, PhD dissertation, Univ. of Illinois, Urbana, 1976.

D. Craggs & R. Hughes-Jones, On the no-three-in-line problem, *J. Combin. Theory Ser. A*, **20**(1976) 363–364; *MR* **53** #10590.

Hallard T. Croft, Kenneth J. Falconer & Richard K. Guy, Unsolved Problems in Geometry, Springer-Verlag, New York, 1991, §**E5**.

H. E. Dudeney, *The Tribune*, 1906-11-07.

H. E. Dudeney, *Amusements in Mathematics*, Nelson, Edinburgh, 1917, pp. 94, 222.

Achim Flammenkamp, Progress in the no-three-in-line problem, *J. Combin. Theory Ser. A* (submitted).

Martin Gardner, Mathematical Games, *Sci. Amer.*, **226** #5 (May 1972) 113–114; **235** #4 (Oct 1976) 133–134; **236** #3 (Mar 1977) 139–140.

Michael Goldberg, Maximizing the smallest triangle made by N points in a square, *Math. Mag.*, **45**(1972) 135–144.

R. Goldstein, K. W. Heuer & D. Winter, Partition of S into n triples; solution to Problem 6316, *Amer. Math. Monthly*, **89**(1982) 705–706.

Richard K. Guy, *Bull. Malayan Math. Soc.*, **0**(1952-53) E22.

Richard K. Guy & Patrick A. Kelly, The no-three-in-line problem, *Canad. Math. Bull.*, **11**(1968) 527–531.

R. R. Hall, T. H. Jackson, A. Sudbery & K. Wild, Some advances in the no-

three-in-line problem, *J. Combin. Theory Ser. A*, **18**(1975) 336–341.
Heiko Harborth, Philipp Oertel & Thomas Prellberg, No-three-in-line for seventeen and nineteen, *Discrete Math.*, **73**(1989) 89–90; *MR* **90f**:05041.
P. A. Kelly, The use of the computer in game theory, M.Sc. thesis, Univ. of Calgary, 1967.
Torliev Kløve, On the no-three-in-line problem II, III, *J. Combin. Theory Ser. A*, **24**(1978) 126–127; **26**(1979) 82–83; *MR* **57** #2962; **80d**:05020.
J. Komlós, J. Pintz & E. Szemerédi, A lower bound for Heilbronn's problem, *J. London Math. Soc.*(2) **25**(1982) 13–24; *MR* **83i**:10042.
Andrew M. Odlyzko, J. Pintz & Kenneth B. Stolarsky, Partitions of planar sets into small triangles, *Discrete Math.*, **57**(1985) 89–97; *MR* **87e**:52007.
Carl Pomerance, Collinear subsets of lattice point sequences - an analog of Szemerédi's theorem, *J. Combin. Theory Ser. A*, **28**(1980) 140–149.
K. F. Roth, On a problem of Heilbronn, *J. London Math. Soc.*, **25**(1951) 198–204, esp. p. 204; II, III, *Proc. London Math. Soc.*, **25**(1972) 193–212; 543–549.
K. F. Roth, Developments in Heilbronn's triangle problem, *Advances in Math.*, **22**(1976) 364–385; *MR* **55** #2771.
Wolfgang M. Schmidt, On a problem of Heilbronn, *J. London Math. Soc.*, **4**(1971/72) 545–550.
T. Thiele, *J. Combin. Theory Ser A* (submitted).

F5. 二次剩余;Schur 猜想

素数 p 的**二次剩余**(quadratic residue)是使同余式 $r \equiv x^2 \bmod p$ 有解的非零整数 r. 在区间$[1,p-1]$中有$\frac{1}{2}(p-1)$个二次剩余,如果 p 是形如 $4k+1$ 的素数,则二次剩余是对称分布的. 如果 $p=4k-1$,则在区间$[1,2k-1]$中比在$[2k,4k-2]$中有更多的二次剩余,但是所有已知的证明都用到 Dirichlet 的类数公式. 对此是否有一个初等证明呢?

对前面一些 d 的值,容易记住哪些素数以 d 作为它的二次剩余:

$d=-1, p=4k+1,$

$d=-2, p=8k+1,3,$ $\qquad d=2, p=8k\pm1,$

$d=-3, p=6k+1,$ $\qquad d=3, p=12k\pm1,$

$d=-5, p=20k+1,3,7,9,$ $\qquad d=5, p=10k\pm1,$

$d=-6, p=24k+1,5,7,11,$ $\qquad d=6, p=24k\pm1,5.$

然而,这恰好是强小数法则的一个例子:在这些小的情形,二次剩余恰好是那些在前一半中的剩余类,或者是在这个剩余系的位于两端处的那四分之一剩余类中,这要按照 d 的符号而定. Legendre 符号(Legendre symbol)$\left(\frac{a}{p}\right)$常用来表示一个与 p 互素的数 a(即 $a\perp p$)的二次特征. 它的值是 ±1,按照 a 是或不是 p 的二次剩余而定. 例如,$\left(\frac{-1}{p}\right)=\pm1$,按照 $p=4k\pm1$ 而定. 这个符号的重要性质是:如果 $a\equiv c \bmod p$,则有 $\left(\frac{a}{p}\right)=\left(\frac{c}{p}\right)$;Gauss 著名的**二次互倒律**(quadratic reciprocity law)是说:对奇素数 p 和 q 有 $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$,除非 p 和 q 两者都是模 4 余 -1 的素数,在此情形有 $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$. 这些结论可以用来对相当大的数的二次特征做快速计算. 例如

$$\left(\frac{173}{211}\right)=\left(\frac{211}{173}\right)=\left(\frac{38}{173}\right)=\left(\frac{2}{173}\right)\left(\frac{19}{173}\right)$$
$$=-\left(\frac{19}{173}\right)=-\left(\frac{173}{19}\right)=-\left(\frac{2}{19}\right)=+1,$$

事实上有 $173\equiv54^2 \bmod 211$.

Legendre 符号的一个有用的推广是 Jacobi 符号(Jacobi Symbol)$\left(\frac{a}{b}\right)$,它是对 $a\perp b$ 和任何正奇数 b 由 Legendre 符号的乘积

$$\prod\left(\frac{a}{p_i}\right)$$

来定义的,这里 $b=\prod p_i$ 是 b 的素因子分解(按重数计算). 它与 Legendre 符号有类似的性质,但要注意:如果 b 不是素数,那么 $\left(\frac{a}{b}\right)=+1$ 不一定蕴含 a 是 b 的二次剩余.

如果 R(或 N)是一个奇素数模 p 的连续的二次剩余(或连续的二次非剩余)的最大个数,那么 A. Brauer 证明了:对 $p\equiv3 \bmod 4$ 有 $R=N<\sqrt{p}$. 另一方面,如果 $p=13$,则 $N=4>\sqrt{13}$,因为 5,

6,7,8 全都是 13 的非剩余. Schur 猜想：如果 p 足够大，则 $N < \sqrt{p}$. Hudson 证明了 Schur 的猜想，此外，他相信 $p = 13$ 是仅有的例外.

参考文献

A. Brauer, Über die Verteilung der Potenzreste, *Math. Z.*, **35**(1932) 39–50; *Zbl.* **3**, 339.

H. Davenport, *The Higher Arithmetic*, Fifth edition, Cambridge University Press, 1982, pp.74–77.

Richard H. Hudson, On sequences of quadratic nonresidues, *J. Number Theory*, **3**(1971) 178–181; *MR* **43** #150.

Richard H. Hudson, On a conjecture of Issai Schur, *J. reine angew. Math.*, **289**(1977) 215–220; *MR* **58** #16481.

F6. 二次剩余的类型

何种类型的二次剩余必定会出现？容易看出总会有一对相邻的二次剩余出现，这是因为 2,5 和 10 中至少有一个是二次剩余，因此(1,2)，(4,5)或(9,10)就是这样一对相邻的二次剩余. 同样地，(1,3)，(2,4)或(4,6)中至少有一对是相差为 2 的二次剩余；(1,4)是一对相差为 3 的二次剩余；(1,5)，(4,8)，(6,10)或(12,16)中至少有一对是相差为 4 的二次剩余；如此等等.

设 $r, r+a, r+b$ 中每个数都是模 p 的二次剩余. Emma Lehmer 问：对什么样的数对(a,b)，对所有充分大的 p 都有这样的三数组出现，这三个数都是 p 的二次剩余呢？用 $\Omega(a,b)$来表示满足如下条件的最小整数：对所有 $p > p(a,b)$，能确保在 $r \leqslant \Omega(a,b)$之内有这样的三数组出现；又当不存在这样一个有限的数时，就记$\Omega(a,b)=\infty$. 例如，Emma Lehmer 证明了 $\Omega(1,2)=\infty$，更一般地还证明了：如果$(a,b)\equiv(1,2) \bmod 3$，或者如果$(a,b)\equiv(1,3),(2,3),(2,4) \bmod 5$，或者如果$(a,b)\equiv(1,5),(2,3),(4,6) \bmod 7$，则有 $\Omega(a,b)=\infty$. 在所有其他情形 $\Omega(a,b)$都是有限的吗？Emma Lehmer 猜想：如果 a 和b 是平方数，那么 $\Omega(a,b)$是有

限的．当然，如果 a 和 b 都比一个平方数少 1，那么有 $\Omega(a,b)=1$．作为例子，让我们来看为何有 $\Omega(5,23)=16$．如果三数组(1,6,24)和(4,9,27)并不全是二次剩余，那么 6 和 3 也不是，而 2 必为剩余．如果三数组(2,7,25)和(13,18,36)并不全是剩余，那么 7 和 13 必为非剩余．在这些情况下，对 $1\leqslant r\leqslant 15$，$(r,r+5,r+23)$ 不一定全是剩余，但当 $r=16$ 时，(16,21,39)是剩余．

表 9 包含了相信是 $\Omega(a,b)$ 的(最小)值．它们对除了已经提到的情形之外的所有情形，都对猜想的 $\Omega(a,b)$ 的有限性提供了有说服力的证据．可否用 a 和 b 给出 $\Omega(a,b)$ 的上界呢?

关于四个二次剩余 $r,r+a,r+b,r+c$ 的类型有何种结论? 当然，如果由其中 3 个剩余类组成的全部 4 个子类型中有任何一个不能保证出现的话，那么这种类型的 4 个剩余类也不一定会出现．我们只需要检查 $(a,b,c)=(2,5,6),(1,6,7),(1,4,9),(5,6,9),(1,6,10),(1,7,10),\cdots$，其中 $\Omega(a,b)$，$\Omega(a,c)$，$\Omega(b,c)$ 和 $\Omega(b-a,c-a)$ 中的每一个都已知是有限的．$\Omega(a,b,c)$ 的某些对应的值是 $\Omega(1,4,9)=357$，$\Omega(1,4,15)=675$，当然还有 $\Omega(3,8,15)=1$．

虽然有 $\Omega(1,6)=24$，$\Omega(1,7)=38$，$\Omega(5,6)=49$，$\Omega(6,7)=57$，但是似乎有 $\Omega(1,6,7)=\infty$．事实上，适合 $(a,b,c,d)=(1,6,7,10)$ 的类型 $r,r+a,r+b,r+c,r+d$ 是这样一种类型，它使得 5 个由 4 个数组成的子类型的每一个都有 $\Omega(1,6,7)=\Omega(1,6,10)=\Omega(1,7,10)=\Omega(5,6,9)=\Omega(6,7,10)=\infty$．

习惯上定义 k-次幂剩余(k-th power residue)是使 $x^k\equiv r \bmod p$ 有解的数 r，它仅对适合 k 整除 $p-1$ 的那种素数有解．同样地我们注意到：每一个大于 10 的素数都有一对不超过数对(9,10)的连续的二次剩余．Hildebrand 证明了：对每个 k 存在一个固定的界 $\Lambda(k,2)$，使得每个充分大的素数都有一对不超过这个界限的连续的 k 次幂剩余．而对 3 个连续的 2 次剩余或 4 次剩余等等，都不存在这样的界．其论据在于让形如 $3k+1$ 的素数成为剩余，而让形如 $3k+2$ 的素数成为非剩余．类似地，取 2 作为剩余，

表 9 $\Omega(a,b)$的值()$a<b\leqslant 25$

a	$b=4$	5	6	7	8	9	10	11	12	13	14
1	45	∞	24	38	∞	84	26	∞	∞	∞	∞
2	∞	25	20	∞	∞	∞	∞	70	30	∞	∞
3	174	39	∞	∞	1	∞	55	∞	∞	36	105
4		∞	∞	∞	∞	91	36	∞	∞	∞	∞
5			49	∞	∞	121	∞	25	4	∞	28
6				57	∞	33	28	∞	24	∞	42
7					∞	∞	75	∞	74	∞	∞
8						66	∞	∞	∞	∞	26
9							∞	54	∞	55	66
10								∞	60	85	∞
11									28	∞	119
12										∞	∞
13											∞

a	$b=15$	16	17	18	19	20	21	22	23	24	25
1	77	35	∞	∞	∞	∞	15	35	∞	21	69
2	54	∞	∞	∞	∞	25	98	∞	∞	∞	∞
3	1	∞	∞	18	36	95	∞	∞	∞	1	51
4	126	60	∞	38	168	∞	90	∞	∞	60	77
5	∞	∞	64	110	∞	100	4	∞	16	64	∞
6	60	36	38	∞	62	78	60	78	∞	45	∞
7	27	9	∞	∞	∞	∞	70	42	∞	∞	45
8	1	∞	∞	77	∞	48	∞	∞	42	1	∞
9	57	66	∞	36	27	16	72	∞	21	∞	119
10	55	∞	∞	32	102	∞	77	26	∞	28	56
11	49	∞	39	∞	∞	∞	64	∞	∞	25	∞
12	∞	65	98	∞	∞	36	4	∞	∞	∞	90
13	42	∞	∞	∞	36	∞	∞	∞	∞	36	∞
14	49	∞	∞	42	∞	52	56	∞	64	81	∞
15		66	27	69	∞	49	25	99	110	1	105
16			∞	∞	102	∞	169	95	∞	∞	56
17				∞	∞	76	64	∞	∞	∞	∞
18					50	∞	∞	∞	62	192	144
19						∞	33	∞	∞	36	96
20							74	∞	40	25	∞
21								93	∞	70	100
22									∞	∞	98
23										∞	∞
24											63

而让所需要的那么多个奇素数成为非剩余，则不存在这样的界，使得对任何 k，在此界限之内会有 4 个连续的 k 次幂剩余出现，这就使得对奇数 k 仅剩下 3 个连续 k 次幂剩余的问题没有解决. $k=3$ 的情形是由 D. H. Lehmer，Emma Lehmer，Mills 和 Selfridge 解决的.

参考文献

Alfred Brauer, Combinatorial methods in the distribution of kth power residues, in *Probability and Statistics*, **4**, University of North Carolina, Chapel Hill, 1969, 14–37.

Adolf Hildebrand, On consecutive k-th power residues, *Monatsh. Math.*, **102** (1986) 103–114; *MR* **88a**:11089.

Adolf Hildebrand, On consecutive k-th power residues II, *Michigan Math. J.*, **38** (1991) 241–253; *MR* **92d**:11097.

D. H. Lehmer & Emma Lehmer, On runs of residues, *Proc. Amer. Math. Soc.*, **13**(1962) 102–106; *MR* **25** #2035.

D. H. Lehmer, Emma Lehmer & W. H. Mills, Pairs of consecutive powerresidues, *Canad. J. Math.*, **15**(1963) 172–177; *MR***26** #3660.

D. H. Lehmer, Emma Lehmer, W. H. Mills & J. L. Selfridge, Machine proof of a theorem on cubic residues, *Math. Comput.*, **16**(1962) 407–415; *MR* **28** #5578.

René Peralta, On the distribution of quadratic residues and nonresidues modulo a prime number, *Math. Comput.*, **58**(1992) 433–440; *MR* **93c**:11115.

F7. 与 Pell 方程类似的三次方程

Hugh Williams 发现，如果 $p\equiv 3 \bmod 4$，那么仅当同余式 $w^2\equiv 2 \bmod p$ 有解，也即 $\left(\frac{2}{p}\right)=1$ 时，方程 $x^2-py^2=2$ 有整数解. 他希望对 $p\not\equiv\pm 1 \bmod 9$ 的情形能给出一个 3 次的类似：仅当 $w^3\equiv 3 \bmod p$ 可解时，方程 $x^3+py^3+p^2z^3-3pxyz=3$ 可解. Barrucand 和 Cohn 证明了这对 $p\equiv 2,5 \bmod 9$ 为真. 对 $p\equiv 4,7 \bmod 9$ 是否为真呢？这是 Barrucand 的一个更一般的猜想的特殊情形. 如果猜想为真，它对于化简 3 次域 $Q(\sqrt[3]{p})$ 的基本单位（正则子）的计算会有用处.

参考文献

P.-A. Barrucand & Harvey Cohn, A rational genus, class number divisibility and unit theory for pure cubic fields, *J. Number Theory*, **2**(1970) 7-21.

H. C. Williams, Improving the speed of calculating the regulator of certain pure cubic fields, *Math. Comput.*, **35**(1980) 1423–1434.

F8. 差为二次剩余的二次剩余

Gary Ebert 要我们求出最大的一组二次剩余 $r_i \bmod p^n$（给定 $p^n \equiv 1 \bmod 4$），使得对所有数对(i,j)，$r_i - r_j$ 都是二次剩余.

F9. 原　　根

素数 p 的一个**原根 g**(primitive root)是一个使 $g, g^2, \cdots, g^{p-1}=1$ 的剩余类全不相同的数. 例如，5 是 23 的原根，因为

$$5,\ 5^2 \equiv 2,\ 5^3 \equiv 10,\ 4,\ -3, 8,\ -6,\ -7, 11, 9,\ -1,$$
$$-5,\quad -2,\quad -10,\ -4, 3,\ -8, 6, 7,\ -11,\ -9, 1$$

对模 23 都属于不同的剩余类.

Artin 有一个著名的猜想：对每一个整数 $g \neq -1$（g 不是平方数），存在无穷多个素数 p 以 g 作为原根. Hooley 在广义 Riemann 猜想为真的条件下证明了这一猜想，Gupta 和 Murty 无条件地证明了它对无穷多个 g 成立. Heath-Brown 证明了如下惊人的定理：除了至多两个例外的素数 p_1, p_2 之外，对每个素数 p，存在无穷多个素数 q 以 p 为其原根. 例如，存在无穷多个素数 q 以 2,3,5 中至少一个作为它的原根.

Erdös 问：如果 p 足够大，是否总有一个素数 $q<p$，使 q 是 p 的一个原根？

给定一个素数 $p>3$，Brizolis 问：是否总有 p 的一个原根 g 以及 $x(0<x<p)$，使有 $x \equiv g^x \bmod p$？果如此，g 可以被选取得满足 $0<g<p$ 和 $g \perp (p-1)$ 吗？

Vegh 问:对所有素数 $p>61$,是否每个整数都可以表为 p 的两个原根之差? W. Narkiewicz 注意到:对 $p>10^{19}$ 答案是肯定的,因而从理论上讲,这个问题可以用计算机来给出解答.

如果 p 和 $q=4p^2+1$ 两者都是素数,Gloria Gagola 问:对所有 $p>3$,3 是否都是 q 的原根? $p=193$ 是否是使得 2 不是 q 的原根的惟一的奇素数? $p=653$ 是否是使得 5 既不是 q 的二次剩余又不是它的原根的惟一的素数? 存在一个数(它可能是 p 的一个函数,例如像 $2p-1$ 这样)总是 q 的一个原根吗?

D. H. Lehmer 和 Emma Lehmer 验证了:对所有形如 n^2+108 的素数 $p<2\cdot 10^8$,6 都是它的原根.(译者注:这句话有误. Wieb Bosma 发现,对 $n=83$,6 不是 $p=n^2+108$ 的原根;John L. Drost 也发现,6 是 6997 的 11 次幂剩余,6 不是以下诸数的原根: $225733=475^2+108$, $237277=487^2+108$, $261229=511^2+108$, $366133=605^2+108,\cdots$)

参 考 文 献

Anton Dumitziu, Congruences du premier degré, *Rev. Roumaine Math. Pures Appl.*, **10**(1965) 1201–1234.

Rajiv Gupta & Maruti Ram Murty, A remark on Artin's conjecture, *Invent. Math.*, **78**(1984) 127–130; *MR* **86d**:11003.

D. R. Heath-Brown, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford Ser.*(2) **37**(1986) 27–38; *MR* **88a**:11004.

C. Hooley, On Artin's conjecture, *J. reine angew. Math.*, **225**(1967) 209–220; *MR* **34** #7445.

Leo Murata, On the magnitude of the least primitive root, *Astérisque No.* **198-200**(1991) 253–257.

Maruti Ram Murty & Seshadri Srinivasan, Some remarks on Artin's conjecture, *Canad. Math. Bull.*, **30**(1987) 80–85; *MR* **88e**:11094.

Michael Szalay, On the distribution of the primitive roots of a prime, *J. Number Theory*, **7**(1975) 184–188; *MR* **51** #5524.

Emanuel Vegh, Pairs of consecutive primitive roots modulo a prime, *Proc. Amer. Soc.*, **19**(1968) 1169–1170; *MR* **37** #6240.

Emanuel Vegh, Primitive roots modulo a prime as consecutive terms of an arithmetic progression, *J. reine angew. Math.*,**235**(1969) 185–188; II, **244**(1970) 185–188; III, **256**(1972) 130–137; *MR* **39** #4086; **42** #1755; **46** #7137.

Emanuel Vegh, A note on the distribution of the primitive roots of a prime, *J. Number Theory*, **3**(1971) 13–18; *MR* **44** #2694.

F10. 2^n 的剩余

Graham 问到 2^n 关于模 n 的剩余. $2^n \equiv 1 \bmod n$ 没有适合 $n>1$ 的解. 只要 n 是一个以 2 为底的伪素数(见 A12)或是一个素数,就有 $2^n \equiv 2 \bmod n$. D. H. Lehmer 和 Emma Lehmer 证明了 $2^n \equiv 3 \bmod n$ 的最小解是 $n = 4700063497 = 19 \cdot 47 \cdot 5263229$. 当然, n 必须是合数,且不被 2 或 3 整除. 事实上,Mąkowski(见 B5 处的参考文献)注意到,如果 $\left(\frac{2}{p}\right)$ 与 $\left(\frac{3}{p}\right)$ 有相反的符号,即如果 $p = 24k \pm 7$ 或 ± 11,那么 n 就不被 p 整除.

Rotkiewicz(与 A12 比较)注意到,如果 m 满足 $2^m \equiv 3 \bmod m$, 那么 $n = 2^m - 1$ 是 $2^{n-2} \equiv 1 \bmod n$ 的一个解.

Benkoski 问: $2^n \equiv 4 \bmod n$ 是否有一个解,当这个解用十进制写出时,最末的那个数字不是 7? 当 $n \equiv 1$ 或 $3 \bmod 10$ 时张明志(Zhang Ming-Zhi)给出了解,他问在 $n \equiv 9 \bmod 10$ 时是否有解.

Victor Meally 报告说:对 $n = 3^k$ 有 $2^n \equiv -1 \bmod n$, 对 $n = 2, 6, 66, 946, \cdots$ 有 $2^n \equiv -2 \bmod n$. Schinzel 发现:存在无穷多个 n 使 $2^n \equiv -2 \bmod n$ 成立这一结论的证明是在 Sierpiński 的 *Elementary Theory of Numbers*(《初等数论》)一书英文版第二版(1987 年)p.235的习题 4 的注解中给出的.

参 考 文 献

Zhang Ming-Zhi, A note on the congruence $2^{n-2} \equiv 1 \bmod n$ (Chinese. English summary), *Sichuan Daxue Xuebao*, **27** (1990) 130–131; *MR* **92b**: 11003 (where the wrong Benkoski reference appears to be given).

F11. 阶乘的剩余之分布

$1!, 2!, 3!, \cdots, (p-1)!, p! \bmod p$ 的分布如何? 大约有

p/e 个剩余类没有被表示出来. 对前面一些 p,它们没有表出的剩余类是:

$p=2$ 或 3,没有未表出的剩余类.

$p=5,\{-2\}$. $p=7,\{-2,-3\}$.

$p=11,\{-2,\pm3,\pm4\}$.

$p=13,\{-3,4,-5\}$.

$p=17,\{4,5,-6,-7,-8\}$.

$p=19,\{3,-5,-6,\pm7,\pm8\}$.

$p=23,\{-3,-4,-6,-7,-8,10\}$.

$p=29,\{-2,-4,7,-8,-9,-10,-11,-12,13,-14\}$.

$p=31,\{\pm3,4,8,\pm10,11,12,13,14\}$.

$p=37,\{3,4,\pm5,-9,10,11,-14,\pm15,-18\}$.

不到最后两个素数,我们或许都会被引导到猜想:未表出的剩余类中负的剩余类的个数至少和正的一样多. 每一种情形都有无穷多个例子吗? $p=23$ 的惊人之处在于:仅有的重复的剩余类是 ±1.

为了回答 Erdös 的一个问题,Rokowska 和 Schinzel 证明了:如果 $2!, 3!, \cdots, (p-1)!$ 代表的剩余类都不相同,那么未表出的剩余类必为 $-\frac{p-1}{2}!$ 所在的剩余类以及 $p\equiv5 \bmod 8$ 所在的类,而在 $5<p\leqslant1000$ 中不存在这样的 p.

参考文献

B. Rokowska & A. Schinzel, Sur une problème de *M*. Erdős, *Elem. Math.*, **15**(1960) 84–85.

R. Stauduhar, Problem 7, *Proc. Number Theory Conf.*, Boulder, 1963, p. 90.

F12. 数与其逆元常有相反的奇偶性吗?

对每个 $x(0<x<p)$,用 $x\bar{x}\equiv1 \bmod p$ 和 $0<\bar{x}<p$ 来定义 $\bar{x}$,这里 p 是一个奇素数. 令 N_p 表示使 x 和 $\bar{x}$ 有相反的奇偶性的那

种情形的个数. 例如,对 $p=13$, $(x,\bar{x})=(1,1)$, $\underline{(2,7)}$, $(3,9)$, $(4,10)$, $\underline{(5,8)}$, $\underline{(6,11)}$, $(12,12)$,从而有 $N_{13}=6$. D. H. Lehmer 要求我们求出 N_p,或者至少得到一些非平凡的结果. 按照 $p\equiv\pm 1\bmod 4$ 分别有 $N_p\equiv 2$ 或 $0\bmod 4$.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61
N_p	0	2	0	4	6	10	4	12	18	4	14	18	20	16	30	32	30

F13. 覆盖同余系

一个同余系 $a_i \bmod n_i$ $(1\leqslant i\leqslant k)$称为是一个覆盖系(covering system),如果每个整数 y 对至少一个 i 的值满足 $y\equiv a_i \bmod n_i$. 例如,0mod 2,0mod 3,1mod 4,5mod 6,7mod 12. 如果 $c=n_1<n_2<\cdots<n_k$,那么 Erdös 悬赏 500 美元给能证明或否定"对任意大的 c 有覆盖同余系存在"这一结论者. Davenport 和 Erdös 以及 Fried 对 $c=3$ 找到了覆盖同余系;Swift 对 $c=6$ 找到了覆盖同余系;Selfridge 对 $c=8$ 找到了覆盖同余系;Churchhouse 对 $c=10$ 找到了覆盖同余系;Selfridge 对 $c=14$ 找到了覆盖同余系;Krukenberg 对 $c=18$ 找到了覆盖同余系;而 Choi 则对 $c=20$ 找到了覆盖同余系.

Erdös 悬赏 25 美元给证明下述结论者:对所有大于 1 的不同的奇数模 n_i,不存在覆盖同余系;而 Selfridge 悬赏 900 美元给提供这样一个同余系的具体例子的人. Berger, Felzenbaum 和 Fraenkel 证明了:这样一个同余系的模的最小公倍数必至少有 6 个素因子. 更一般地,"奇的"可以换成"不被前 r 个素数整除的". Simpson 和 Zeilberger 证明了:如果这些模都是奇的,且无平方因子,那么它们的最小公倍数至少要有 18 个素因子.

Jim Jordan 对能给出有关 Gauss 整数的类似问题(A15)的解答者提供了与上面提到的悬赏金额相当的奖金.

Erdös 注意到,利用 210 的真因子可以对所有大于 1 的不同的无平方因子模 n_i 得到一个覆盖同余系:

a_i	0	0	0	1	0	1	1	2	2	23	4	5	59	104
n_i	2	3	5	6	7	10	14	15	21	30	35	42	70	105

Krukenberg 用到 2 和大于 3 的无平方因子数. Selfridge 问:是否能代替 $c=2$ 而对$c\geqslant 3$得到这样一个覆盖同余系? 他注意到:诸 n_i 不能全是有至多 2 个素因子的无平方因子数,但是上面的例子表明,并不需要多于三个素因子.

对一个有不同模的覆盖系来说,证明 $\sum_{i=1}^{k} 1/n_i > 1$ 是不困难的,但也并非是无聊之举. 如果 $n_1=3$ 或 4 的话,此和可以任意接近 1. Selfridge 和 Erdös 猜想有 $\sum 1/n_i > 1 + c_{n_1}$,其中 c_{n_1}与 n_1 一起趋向无穷.

Schinzel 要求一个覆盖系,其中没有哪个模能整除其他的模. 如果不存在有奇数模的覆盖系的话,则这样的覆盖系也不存在.

Simpson 称一个覆盖系是无冗的(irredundant), 如果从中去掉一个同余类后它不再覆盖整数. 他证明了:如果这样一个同余系所有模的最小公倍数是 $\prod p_i^{\alpha_i}$,那么该同余系至少包含 $1+\sum \alpha_i(p_i-1)$ 个同余类.

Erdös 猜想:所有形如 $d\cdot 2^k+1(k=1,2,\cdots)$的不包含素数的序列都可以从覆盖同余系得到,这里 d 是固定的奇数(例子请见 B21). 等价地说,这样一个序列的元素的最小素因子是无界的.

参考文献

Marc Aron Berger, Alexander Gersh Felzenbaum & A. S. Fraenkel, Necessary conditions for the existence of an incongruent covering system with odd moduli II, *Acta Arith.*, **48**(1987) 73–79.

S. L. G. Choi, Covering the set of integers by congruence classes of distinct moduli, *Math. Comput.*, **25**(1971) 885-895; *MR* **45** #6744.

R. F. Churchhouse, Covering sets and systems of congruences, in *Computers in Mathematical Research*, North-Holland, 1968, 20–36; *MR* **39** #1399.

Fred Cohen & J. L. Selfridge, Not every number is the sum or difference of two prime powers, *Math. Comput.*, **29**(1975) 79–81.

P. Erdős, Some problems in number theory, in *Computers in Number Theory*,

Academic Press, 1971, 405–414; esp. pp. 408–409.

J. Haight, Covering systems of congruences, a negative result, *Mathematika*, **26**(1979) 53–61; *MR* **81e**:10003.

J. H. Jordan, Covering classes of residues, *Canad. J. Math.*, **19**(1967) 514–519; *MR* **35** #1538.

J. H. Jordan, A covering class of residues with odd moduli, *Acta Arith.*, **13**(1967-68) 335–338; *MR* **36** #3709.

C. E. Krukenberg, PhD thesis, Univ. of Illinois, 1971, 38–77.

A. Schinzel, Reducibility of polynomials and covering systems of congruences, *Acta Arith.*, **13**(1967) 91–101; *MR* **36** #2596.

R. J. Simpson, Regular coverings of the integers by arithmetic progressions, *Acta Arith.*, **45**(1985) 145–152; *MR* **86j**:11004.

R. J. Simpson & D. Zeilberger, Necessary conditions for distinct covering systems with squarefree moduli, *Acta Arith.*,**59**(1991) 59–70.

Zhang Ming-Zhi, A note on covering systems of residue classes, *Sichuan Daxue Xuebao* **26**(1989) 185–188; *MR* **92c**:11003.

Stefan Znám, A survey of covering systems of congruences, *Acta Math. Univ. Comen.*, **40-41**(1982) 59–79; *MR* **84e**:10004.

F14. 精确覆盖同余系

如果一个同余系既是覆盖同余系，又是不相交的(每个整数恰好只被一个同余类所覆盖)，它就称为是一个精确覆盖同余系(exact covering system). 一个同余系是精确覆盖同余系的必要而非充分的条件是:对所有 i,j 有 $\sum_{i=1}^{k} 1/n_i = 1$ 以及$(n_i, n_j)>1$，这里的记号如同 F13 中第一句所定义的那样. 有一个各种说法都归功于{Davenport, Mirsky, Newman, Rado}的子集合的定理是说:如果有一组不同的大于 1 的数的集合是同余式的模，那么或者有一个数，它不在任何一个同余类之中;或者有一个数，它在其中不止一个同余类之中. 它的巧妙的证明用到了母函数和单位根. 此后，由 Berger, Felzenbaum 和 Fraenkel，以及 Simpson 给出了组合证明.

正如在第一版中所叙述的，Znám 注意到$(n_1, n_2, \cdots, n_k)>1$ 并不是必要条件，正如例子 0(mod 6)，1(mod 10)，2(mod 15)以及 3,4,5,7,8,9,10,13,14,15,16,19,20,22,23,25,26,27,28,29

(mod 30)所表示出的那样. 他进一步证明了:如果 p 是 n_k 的最小素因子,那么 $n_k = n_{k-1} = \cdots = n_{k-p+1}$. 由此他就证明了 Mycielski 的一个猜想. 他还猜想:如果只有一对相等的模,那么所有的模都形如 $2^\alpha 3^\beta$,但是后来他以及 Burshtein 和 Schönheim, 还有 Joel Spencer 每个人都给出了此猜想的反例,比如

	0, 1	2, 7	3, 8	13, 28	4, 9	14, 34	19, 39	59,119
mod	5	10	15	30	20	40	60	120.

Stein 证明了:如果只有单独一对相等的模,而其余的模都不相同,那么 $n_i = 2^i (1 \leqslant i \leqslant k-1)$, $n_k = 2^{k-1}$. 类似地,Znám 证明了:如果有 3 个相等的模,其余的模都不相同,那么 $n_i = 2^i (1 \leqslant i \leqslant k-3)$, $n_{k-2} = n_{k-1} = n_k = 3 \cdot 2^{k-3}$. Beebee 将 Stein 的结果作了推广,他证明了:一个覆盖同余系仅当

$$\sin \pi z = -2^{k-1} \prod_{i=1}^{k} \sin \frac{\pi}{n_i}(a_i - z)$$

成立时才是精确覆盖同余系.

Simpson 推广了 Burshtein 和 Schönheim 的工作,他证明了:如果素数 $p_1 < p_2 < \cdots < p_t$ 是整除一个精确覆盖同余系的模的那些素数,在该同余系中没有哪个模能出现多于 N 次,那么

$$p_t \leqslant N \prod_{i=1}^{t-1} \frac{p_i}{p_i - 1}.$$

最主要的问题是刻画精确覆盖同余系的特征.

Porubsky 问:是否有一个"m 次精确覆盖同余系",它不是 m 个精确覆盖同余系的并集? 更为一般地,称这样一个同余系 S 是**可约的**(reducible),如果存在一个分化 $S = S_1 \cup S_2$,使得对某个 $l(0 < l < m)$, S_1 和 S_2 恰好分别是 l 次和 $m-l$ 次的精确覆盖同余系;又称这样一个同余系 S 是不可约的(irreducible),如果不存在这样一个分化. 张明志(Zhang Ming-Zhi)对 Porubsky 的问题给出了肯定的回答,他证明了:对每个 $m > 1$,存在一个不可约的 m 次精确覆盖同余系. 对 $m = 2$ 此结论已被 S. L. G. Choi (Keszthely, 1973)和 Zeilberger 所证明,例如:

$$1(2);0(3);2(6);0,4,6,8(10);$$
$$1,2,4,7,10,13(15);5,11,12,22,23,29(30).$$

可能存在所有的模都不相同的无限不相交的精确覆盖同余系. 如果该同余系所有模的倒数之和等于 1,则对模 $\{2,2^2,2^3,\cdots\}$ 以及对一组形如 $2^\alpha 3^\beta$ 的模存在这样的同余系. Fraenkel 和 Simpson 猜想这些是仅有的存在无限精确覆盖同余系的情形. Lewis 证明了:仅有的可能的例外是有一组无穷多个素数整除它们的模的情形.

可以对 Beatty 序列(E27)的覆盖同余系提出问题. Graham 证明了:如果

$$\lfloor m\alpha_i + \beta_i \rfloor;\ m \in \mathbb{Z};\ 1 \leqslant i \leqslant k$$

是这样一个同余系($k>2$),且至少有一个 α_i 是无理数,那么必有某两个 α_i 相等. 但如果所有的 α_i 都是有理数,这未必成立,这是因为

$$\left\lfloor m\,\frac{2^k-1}{2^{k-i}} + 1 - 2^{i-1} \right\rfloor \quad (1 \leqslant i \leqslant k)$$

是精确覆盖同余系. Fraenkel 猜想:仅有的有不同的 α_i 的这种同余系必有这种形式.

它们与伪完全数(B2)以及埃及分数(D11)有联系.

参考文献

John Beebee, Examples of infinite, incongruent exact covers, *Amer. Math. Monthly*, **95**(1988) 121–123; errata **97**(1990) 412; *MR*, **89g**:11013, **91a**:11013.

John Beebee, Some trigonometric identities related to exact covers, *Proc. Amer. Math. Soc.*, **112**(1991) 329–338; *MR*, **91i**:11013.

John Beebee, Bernoulli numbers and exact covering systems, *Amer. Math. Monthly*, **99**(1992) 946–948; *MR* **93i**:11025.

Marc Aron Berger, Alexander Gersh Felzenbaum & A. S. Fraenkel, A non-analytic proof of the Newman-Znám result for disjoint covering systems, *Combinatorica*, **6**(1986) 235–243.

Marc Aron Berger, Alexander Gersh Felzenbaum, A. S. Fraenkel & R. Holzman, On infinite and finite covering systems, *Amer. Math. Monthly*, **98**(1991) 739–742; *MR* **92g**:11009.

N. Burshtein, On natural exactly covering systems of congruences having moduli occurring at most N times, *Discrete Math.*, **14**(1976) 205–214.

N. Burshtein & J. Schönheim, On exactly covering systems of congruences having moduli occurring at most twice, *Czechoslovak Math. J.*, **24(99)**(1974) 369–372; *MR* **50** #4521.

J. Dewar, On finite and infinite covering sets, in *Proc. Washington State Univ. Conf. Number Theory*, Pullman WA, 1971, 201–206.

P. Erdős, On a problem concerning systems of congruences (Hungarian; English summary), *Mat. Lapok*, **3**(1952) 122–128.

A. S. Fraenkel, The bracket function and complementary sets of integers, *Canad. J. Math.*, **21**(1967) 6–27.

A. S. Fraenkel, Complementing and exactly covering sequences, *J. Combin. Theory Ser. A*, **14**(1973) 8–20; *MR* **46** #8875.

A. S. Fraenkel, A characterization of exactly covering congruences, *Discrete Math.*, 4(1973) 359–366; *MR* **47** #4906.

A. S. Fraenkel, Further characterizations and properties of exactly covering congruences, *Discrete Math.*, **12**(1975) 93–100; erratum 397; *MR* **51** #10276.

A. S. Fraenkel & R. Jamie Simpson, On infinite disjoint covering systems, *Proc. Amer. Math. Soc*, **119**(1993) 5–9; *MR* **93k**:11006.

R. L. Graham, Covering the positive integers by disjoint sets of the form $\{\lfloor n\alpha+\beta\rfloor : n=1,2,\ldots\}$, *J. Combin. Theory Ser. A*, **15**(1973) 354–358; *MR* **48** #3911.

R. L. Graham, Lin Shen & Lin Chio-Shih, Spectra of numbers, *Math. Mag.*, **51**(1978) 174–176; *MR* **58** #10808.

I. Korec, On a generalisation of Mycielski's and Znam's conjectures about coset decomposition of abelian groups, *Fundamenta Math.*, **85**(1974) 41–48.

I. Korec, On number of cosets in nonnatural disjoint covering systems, *Colloq. Math. Soc. János Bolyai* **51** (Number Theory, Vol. 1, Budapest, 1987), North-Holland, 1990, 265–278.

Ethan Lewis, Infinite covering systems of congruences which don't exist, *Proc. Amer. Math. Soc.*, (1993).

Ryozo Morikawa, Some examples of covering sets; On a method to construct covering sets; On eventually covering families generated by the bracket function, *Bull. Fac. Liberal Arts Nagasaki Univ.*, **21**(1981) 1–4; **22**(1981) 1–1; **23**(1982/83) 17–22; *MR* **84j**:10064; **84i**:10057; **84c**:10051.

Ryozo Morikawa, Disjointness of sequences $[\alpha_i n+\beta_i]$, $i=1, 2$, *Proc. Japan Acad. Ser. A Math. Sci.*, **58**(1982) 269–271; *MR* **83m**:10096.

Morris Newman, Roots of unity and covering sets, *Math. Ann.*, **191**(1971) 279–282; *MR* **44** #3972 & err. p. 1633.

Břetislav Novák & Štefan Znám, Disjoint covering systems, *Amer. Math. Monthly*, **81** (1974) 42–45.

Štefan Porubský, On m times covering systems of congruences, *Acta Arith.*, **29**(1976) 159–169; *MR* **53** #2884.

Štefan Porubský, Results and problems on covering systems of residue classes, *Mitt. Math. Sem. Giessen*, **150**(1981)85 pp.; *MR* **83j**:10008.

R. J. Simpson, Disjoint covering systems of congruences, *Amer. Math. Monthly*, **94**(1987) 865–868; *MR* **89b**:11006.

R. J. Simpson, Exact coverings of the integers by arithmetic progressions, *Discrete Math.*, **59**(1986) 181–190.

R. J. Simpson, Disjoint covering systems of rational Beatty sequences, *Discrete Math.*, **92**(1991) 361–369.

Sherman K. Stein, Unions of arithmetic sequences, *Math. Ann.*, **134**(1958) 289–294; *MR* **20** #17.

Sun Zhi-Wei, On exactly m times covers, *Israel J. Math.*, **77**(1992) 345–348; *MR* **93k**:11007.

Charles Vanden Eynden, On a problem of Stein concerning infinite covers, *Amer. Math. Monthly*, **99**(1992) 355–358; *MR* **93b**:11004.

Doron Zeilberger, On a conjecture of R. J. Simpson about exact covering congruences, *Amer. Math. Monthly* **96**(1989) 243.

Zhang Ming-Zhi, Irreducible systems of residue classes that cover every integer exactly m times (Chinese, English summary), *Sichuan Daxue Xuebao*, **28**(1991) 403–408; *MR* **92j**:11001.

Štefan Znám, On Mycielski's problem on systems of arithmetical progressions, *Colloq. Math.*, **15**(1966) 201-204; *MR* **34** #134.

Štefan Znám, On exactly covering systems of arithmetic sequences, *Math. Ann.*, **180** (1969) 227-232; *MR* **39** #4087.

Štefan Znám, A simple characterization of disjoint covering systems, *Discrete Math.*, **12**(1975) 89–91; *MR* **51** #12772.

F15. R. L. Graham 的一个问题

Szegedy 由于对下述问题给出了(肯定的)解答而赢得了 Graham 提供的奖金:$0<a_1<a_2<\cdots<a_n$ 是否蕴含 $\max_{i,j} a_i/(a_i, a_j) \geqslant n$? 他的证明和 Zaharescu 的证明都是对充分大的 n 来做的. Cheng Yuanyou 和 Pomerance 给出一个明确的界 10^{4275},但仍然还有相当的空隙需要填补.

参考文献

Cheng Yuanyou & Carl Pomerance, On Graham's conjecture, *Rocky Mountain J. Math.*, (1994) (to appear).

Paula A. Kemp, A conjecture of Graham concerning greatest common divisors, *Nieuw Arch. Wisk.*(4), **8**(1990) 61–62; *MR* **91e**:11003.

Rivka Klein, The proof of a conjecture of Graham for sequences containing

primes, *Proc. Amer. Math. Soc.*, **95**(1985) 189–190; *MR* **86k**:11002.

J. W. Sander, On a conjecture of Graham, *Proc. Amer. Math. Soc.*, **102**(1988) 455–458; *MR* **89c**:11004.

R. J. Simpson, On a conjecture of R. L. Graham, *Acta Arith.*, **40**(1981/82) 209–211; *MR* **83j**:10062.

M. Szegedy, The solution of Graham's greatest common divisor problem, *Combinatorica*, **6**(1986) 67–71; *MR* **87i**:11010.

Alexandru Zaharescu, On a conjecture of Graham, *J. Number Theory*, **27** (1987) 33–40; *MR* **88k**:11009.

F16. 整除 n 的小素数幂的乘积

Erdös 定义 $A(n,k)$ 为 $\prod p^a$，这里的乘积取过小于 k 且满足 $p^a \| n$ 的素数 p，他问是否有

$$\max_n \min_{1\leqslant i\leqslant k} A(n+i,k) = o(k)?$$

他指出不难证明它等于 $O(k)$. 对每个 c 和充分大的 k 是否有

$$\min_n \max_{1\leqslant i\leqslant k} A(n+i,k) > k^c?$$

是否有

$$\sum_{i=1}^{k} \frac{1}{A(n+i,)} > c\ln k?$$

F17. 与 ζ 函数有关的级数

Alf van der Poorten 在和其他人证明

$$\frac{1}{2}\sum_{n=1}^{\infty} \frac{1}{n^4\binom{2n}{n}} = \int_0^{\frac{\pi}{3}} \theta\left(\ln 2 \sin\frac{\theta}{2}\right)^2 d\theta = \frac{17\pi^4}{6480}$$

之前曾要求给出

$$\zeta(4)\left[= \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}\right] = \frac{36}{17}\sum_{n=1}^{\infty} \frac{1}{n^4\binom{2n}{n}}$$

的一个证明.

已知

$$\sum_{n=1}^{\infty} \frac{1}{\binom{2n}{n}} = \frac{2\pi\sqrt{3}+9}{27}, \quad \sum_{n=1}^{\infty} \frac{1}{n\binom{2n}{n}} = \frac{\pi\sqrt{3}}{9},$$

$$\zeta(2)\left[=\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}\right] = 3\sum_{n=1}^{\infty} \frac{1}{n^2\binom{2n}{n}},$$

$$2(\sin^{-1}x)^2 = \sum_{n=1}^{\infty} \frac{(2x)^{2n}}{n^2\binom{2n}{n}}$$

以及

$$\zeta(3)\left[=\sum_{n=1}^{\infty} \frac{1}{n^3}\right] = \frac{5}{2}\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^3\binom{2n}{n}}.$$

Gosper 发现了一些惊人的恒等式,其中包括

$$\sum_{k\geqslant 1} \frac{30k-11}{4(2k-1)k^3\binom{2k}{k}^2} = \zeta(3),$$

$$\sum_{n\geqslant 1} \frac{2^{-n}}{1+x^{2^{-n}}} = \frac{1}{\ln x} + \frac{1}{1-x}.$$

参考文献

Louis Comtet, *Advanced Combinatorics*, D. Reidel, Dordrecht, 1974, p. 89.

John A. Ewell, A new series representation for $\zeta(3)$, *Amer. Math. Monthly*, **97**(1990) 219–220; *MR* **91d**:11103.

R. William Gosper, Strip mining in the abandoned orefields of nineteenth century mathematics, *Computers in Mathematics* (Stanford CA, 1986), *Lecture Notes in Pure and Appl. Math.*, Dekker, New York, **125**(1990) 261–284.

Leonard Levin, *Polylogarithms and Associated Functions*, North-Holland, 1981 [§7.62, and foreword by van der Poorten].

Alfred van der Poorten, A proof that Euler missed ... Apery's proof of the irrationality of $\zeta(3)$, *Math. Intelligencer*, **1**(1979) 195–203.

Alfred J. van der Poorten, Some wonderful formulas ... an introduction to polylogarithms, *Proc. Number Theory Conf.*, Queen's Univ., Kingston, 1979, 269–286; *MR* **80i**:10054.

F18. 一个集合的元素的和与积组成的集合之大小

如果 $a_1, a_2, \cdots, a_n$ 是 n 个数(不一定是整数),它们两两的和与两两的积组成的集合有多大? 是否有

$$¿\quad \left| \{a_i + a_j\} \cup \{a_i a_j\} \right| > n^{2-\epsilon} \quad ?$$

Erdös 和 Szemerédi 证明了:这个集合的基数大于 n^{1+c_1} 且小于 $n^2 \exp(-c_2 \ln n / \ln \ln n)$.

参 考 文 献

P. Erdős, Some recent problems and results in graph theory, combinatorics and number theory, *Congress. Numer.*, **17** Proc. 7th S.E. Conf. Combin. Graph Theory, Comput., Boca Raton, 1976, 3–14 (esp. p. 11).

P. Erdős & E. Szemerédi, On sums and products of integers, *Studies in Pure Mathematics*, Birkhäuser, 1983, pp. 213–218; *MR* **86m**:11011.

F19. 将数分成有最大乘积的不同素数之和

在第一版里我们问道:如果 n 很大,且用任何可能的方式写成形式 $n = a + b + c (0 < a < b < c)$,是否所有的乘积 abc 都不相同? 但是 Leech 发现 D16 对此作了否定的回答. 也见 Kelly 的论文. 代替乘积,改为考虑让最小公倍数取最大值这一类似的问题,则由 Drago 从算法上对此进行了研究.

J. Riddell 和 H. Taylor 问:在把 n 分成不同素数之和的分化之中,使各部分的乘积有最大值的那个分化是否一定是使分化出的各部分的个数最多的那个分化? 但 Selfridge 对此给出了否定的回答,他给出例子

$$\begin{aligned} 319 &= 2 + 3 + 5 + 7 + 11 + 13 + 17 + 23 \\ &\quad + 29 + 31 + 37 + 41 + 47 + 53 \\ &= 3 + 5 + 11 + 13 + 17 + 19 + 23 + 29 \\ &\quad + 31 + 37 + 41 + 43 + 47, \end{aligned}$$

而本例中是分化成的部分的个数较少的那个分化给出了最大可能

的乘积. 这是否是最小的反例? 两个集合的基数之差能否任意大?

参 考 文 献

Antonino Drago, Rules to find the partition of n with maximum l.c.m., *Atti Sem. Mat. Fis. Univ. Modena*, **16**(1967) 286-298; *MR* **37** #180.

J. B. Kelly, Partitions with equal products, *Proc. Amer. Math. Soc.*, **15**(1964) 987-990.

F20. 连 分 数

数 x 可以表示成连分数(continued fraction)

$$x = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cdots}}},$$

为方便打印,它常写成

$$x = a_0 + \frac{b_1}{a_1 +} \frac{b_2}{a_2 +} \frac{b_3}{a_3 +} \cdots.$$

当分子 b_i 全都是 1 时,称之为简单连分数(simple continued fraction),它可以写成

$$x = [a_0; a_1, a_2, a_3, \cdots].$$

简单连分数可以是有限的,也可以是无限的,但是当 x 为有理数时它是有限的. 在此情形它有两种可能的形式,在其中一种形式里它最后一个**部分商**(partial quotient)a_k 等于 1:

$$\frac{7}{16} = [0;2,3,2] = [0;2,3,1,1].$$

Zaremba 猜想:给定任何整数 $m>1$,必存在一个整数 a,$0<a<m$,$a \perp m$,使得 a/m 的简单连分数$[0;a_1,\cdots,a_k]$满足 $a_i \leqslant B$(对 $1 \leqslant i \leqslant k$),这里 B 是一个小的绝对常数(比方说 $B=5$). 他只能证明有 $a_i \leqslant C\ln m$.

参考文献

T. W. Cusick, Zaremba's conjecture and sums of the divisor function, *Math. Comput.*, **61**(1993) 171–176.

S. K. Zaremba, La méthode des "bons treillis" pour le calcul des intégrales multiples, in *Applications of Number Theory to Numerical Analysis* (*Proc. Symp. Univ. Montréal*, 1971) Academic Press, 1972, 93–119 esp. 69 & 76; *MR* **49** #8271.

F21. 所有部分商皆为 1 或 2 的连分数

并非每个整数 n 都可以表为这样的两个正整数之和 $n=a+b$,使 a/b 的连分数的所有的部分商都是 1 或 2. 对 11,17 和 19 我们有

$$\frac{4}{7}=[0;1,1,2,1],\quad \frac{5}{12}=[0;2,2,2],$$

$$\frac{7}{12}=[0;1,1,2,2],$$

但是 23 不能如此表示. 不过 Leo Moser 猜想存在一个常数 c,使得每个 n 都可以这样来表示:它的部分商之和 $\sum a_i < c\ln n$.

Bohuslav Divis 要求给出下述结论一个证明:在任何实二次域中,总有一个无理数的连分数展开式的所有部分商都是 1 或 2. 他还对用任一对不同的正整数代替 1 和 2 的情形提出了同样的问题.

F22. 部分商无界的代数数

是否存在次数大于 2 的代数数,它的连分数有无界的部分商?每个这样的数都有无界的部分商吗? Ulam 特别问到数 $\xi/(\xi+y)$,这里 $y=1/(1+y)$.

Littlewood 注意到,如果 θ 的连分数有无界的部分商 a_n,那么 $\liminf n|\sin n\theta|\leqslant A(\theta)$,其中 $A(\theta)$不是 0(尽管对几乎所有的 θ 而言这是对的). 他还问是否对所有实的 θ 和 ϕ 都有

$$\liminf n\,|\sin n\theta \sin n\phi| = 0?$$

对几乎所有 θ 和 ϕ 而言这个结果是对的. Cassels 和 Swinnerton-Dyer 处理了一个对偶的问题,并附带证明了:$\theta=2^{1/3}$ 和 $\varphi=4^{1/3}$没有给出反例. Davenport 建议说,用计算机或许可以帮助我们证明:比方说当 $\epsilon=\frac{1}{10}$或$\frac{1}{50}$时

$$|(x\theta-y)(x\varphi-z)|<\epsilon$$

对每个 θ 和 φ 都有解.

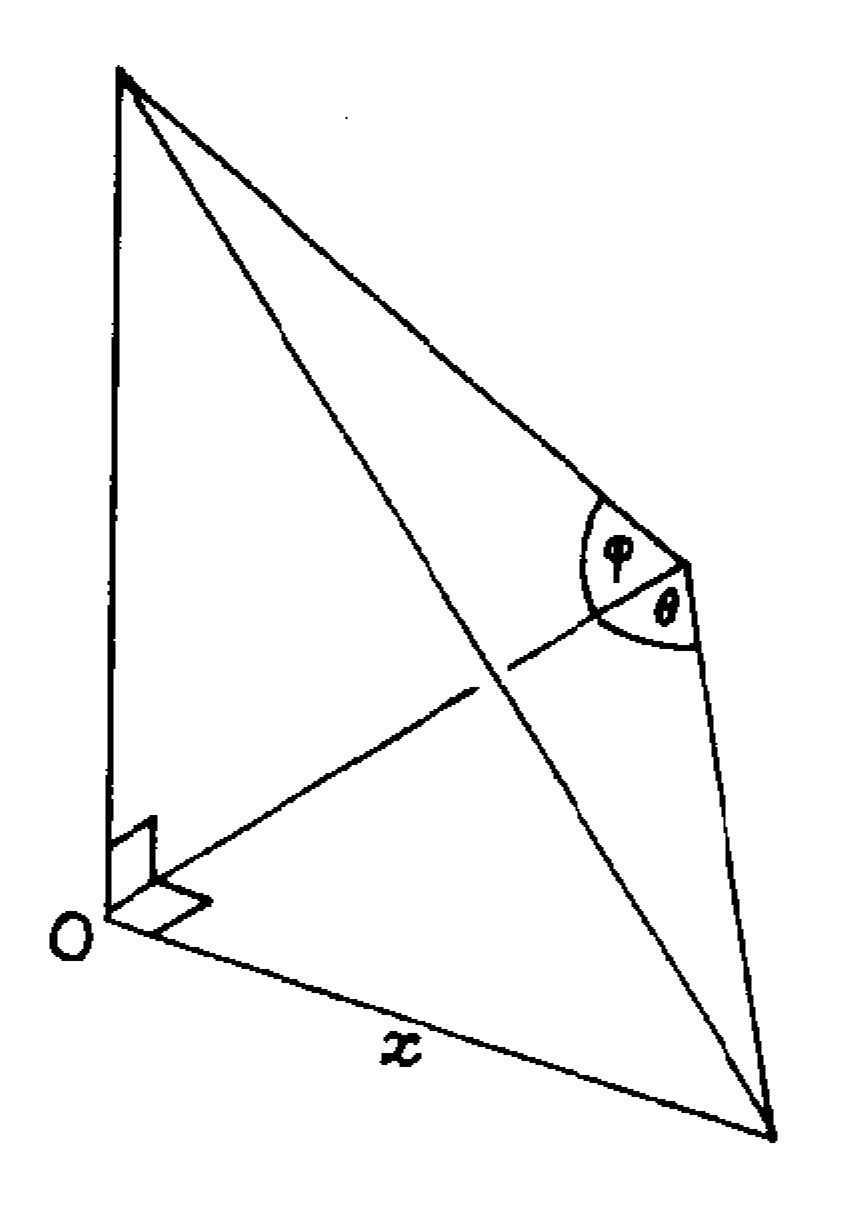


图 18 直四面体

参考文献

J. W. S. Cassels & H. P. F. Swinnerton-Dyer, On the product of three homogeneous linear forms and indefinite ternary quadratic forms, *Philos. Trans. Roy. Soc. London Ser. A*, **248**(1955) 73–96; *MR* **17**, 14.

Harold Davenport, Note on irregularities of distribution, *Mathematika*, **3** (1956) 131–135; *MR* **19**, 19.

John E. Littlewood, *Some Problems in Real and Complex Analysis*, Heath, Lexington MA, 1968, 19–20, Problems 5, 6.

F23. 2 和 3 的幂之间的最小差

Littlewood 的书中的问题 1 问道:与 2^m 相比,3^n-2^m 能有多小? 他给出一个例子

$$\frac{3^{12}}{2^{19}}=1+\frac{7153}{524288}\approx 1+\frac{1}{73}$$

($D^{\#}$ 和 E^{b} 的比值).

log3(以 2 为底)的连分数(见 F20)

$$1+\frac{1}{1+}\frac{1}{1+}\frac{1}{2+}\frac{1}{2+}\frac{1}{3+}\frac{1}{1+}\cdots$$

的前面几个渐进分数是

$$\frac{1}{1},\frac{2}{1},\frac{3}{2},\frac{8}{5},\frac{19}{12},\frac{65}{41},\frac{84}{53},\cdots$$

于是 Victor Meally 发现，八度音程可以被分成 12，41 或 53 个区间，而有 53 度的调律系统属于 Nicolaus Mercator.

Ellison 用 Gel'fond-Baker 方法证明了

$$|2^x - 3^y| > 2^x e^{-x/10} \quad (\text{对 } x > 27),$$

而 Tijdeman 由此证明了：存在一个 $c \geqslant 1$ 使有 $|2^x - 3^y| > 2^x / x^c$.

Croft 对 $n! - 2^m$ 提出了相应的问题. 用 2 的幂对 $n!$ 所给出的前面几个最好的逼近是

5!	20!	22!	24!	61!	63!	90!
2^7	2^{61}	2^{70}	2^{79}	2^{278}	2^{290}	2^{459}
−1.34	+0.13	−0.10	+0.046	+0.023	−0.0017	−0.0007,

其中第三行是关于指数的百分比误差.

在 Benne de Weger 的博士学位论文的"附录"中他注意到，如果给定素数 $p_1, \cdots, p_t$，那么必存在一个可有效计算的常数 C，它只与 p_i 有关，使得对所有满足 $n! \neq p_1^{k_1} \cdots p_t^{k_t}$ 的 $n, k_1, \cdots, k_t$ 有

$$|n! - p_1^{k_1} \cdots p_t^{k_t}| > \exp(Cn/\ln n).$$

猜想此式的右边可以代之以 $\exp(C'n\ln n)$，对此有一些实验数据予以支持. 对固定的 m，这篇博士论文的方法可以确定

$$n! - p_1^{k_1} \cdots p_t^{k_t} = m$$

的所有解.

Erdös 相信此猜想为真. 他还注意到，仅当 $n = 1,2,3,4,5$ 时有 $n! = 2^a \pm 2^b$.

参考文献

F. Beukers, Fractional parts of powers of rationals, *Math. Proc. Cambridge Philos. Soc.*, **90**(1981) 13-20; *MR* **83g**:10028.

A. K. Dubitskas, A lower bound on the value of $\|(3/2)^k\|$ (Russian), *Uspekhi Mat. Nauk*, **45**(1990) 153–154; translated in *Russian Math. Surveys*, **45**(1990) 163–164; *MR* **91k**:11058.

W. J. Ellison, Recipes for solving diophantine problems by Baker's method, *Sém. Théorie Nombres*, 1970–71, Exp. No. 11, C.N.R.S. Talence, 1971.

R. Tijdeman, On integers with many small factors, *Compositio Math.*, **26** (1973) 319-330.

F24. 恰有两个不同的十进位数字的平方数

Sin Hitotumatu 要求证明或推翻下述结论：除了 10^{2n}，$4 \cdot 10^{2n}$ 以及 $9 \cdot 10^{2n}$ 之外，仅有有限多个平方数恰由两个不同的十进位数字组成，例如 $38^2 = 1444$，$88^2 = 7744$，$109^2 = 11881$，$173^2 = 29929$，$212^2 = 44944$，$235^2 = 55225$ 以及 $3114^2 = 9696996$.

F25. 数的持续性

在序列 679，378，168，48，32，6 中，每一项都是前一项的十进位数字的乘积. Neil Sloane 把按照上述规则将一个数变成一个个位数所需的步数（在上例中是 5）定义为该数的**持续性**（persistence）. 持续性为 1，2，…，11 的最小的数是 10，25，39，77，679，6788，68889，2677889，26888999，3778888999，277777788888899. 在小于 10^{50} 的数中没有持续性大于 11 的数. Sloane 猜想：存在一个数 d，使得没有哪个数的持续性能大于 d.

在以 2 为基数的数中（即写成二进制数——译者注），数的持续性最大为 1. 在以 3 为基数的数中（即写成 3 进制数——译者注），经过一次这样的变换得到的第二项要么是 0，要么是一个形如 2 的幂的数. 猜想所有大于 2^{15} 的形如 2 的幂的数在写成以 3 为基数的数时必含有一个 0. 这对直到 2^{500} 的数都是对的. 这一猜想如果为真，就会蕴含以 3 为基数的数的最大的持续性是 3.

Sloane 的一般的猜想是：存在一个数 $d(b)$，在以 b 为基数的数中，数的持续性最大不超过 $d(b)$.

Erdös 对问题作了修改，他令 $f(n)$ 是 n 的非 0 的十进位数字之积，并问可以多快达到一位数，又问对什么样的数，它降为一位数的速度最慢？他说容易证明 $f(n) < n^{1-c}$，因此变为一位数最多需要 $c\ln\ln n$ 步.

参 考 文 献

N. J. A. Sloane, The persistence of a number, *J. Recreational Math.*, **6**(1973) 97–98.

F26. 仅用 1 表示数

令 $f(n)$是可以用 1 以及任意多个 + 号和 × 号(以及括号)来表示出 n 时所用的 1 的最少的个数. 例如

$$80 = (1+1+1+1+1)\times(1+1+1+1)\times(1+1+1+1),$$

从而有 $f(80)\leqslant 13$. 可以证明 $f(3^k)=3k$ 且 $3\log_3 n\leqslant f(n)\leqslant 5\log_3 n$,其中的对数以 3 为底. $f(n)\sim 3\log_3 n$ 成立吗?

Daniel Rawsthorne 证明了:当 n 形如 2^a3^b 且不大于 3^{10}时有 $f(n)=2a+3b$. 对更大的这样的 n,它是否仍然为真?

对素数 p,是否总有 $f(p)=1+f(p-1)$成立? 又是否总有 $f(2p)=\min\{2+f(p),1+f(2p-1)\}$?

参 考 文 献

J. H. Conway & M. J. T. Guy, π in four 4's, *Eureka*, **25**(1962) 18–19.

Richard K. Guy, Some suspiciously simple sequences, *Amer. Math. Monthly*, **93**(1986) 186–190; and see **94**(1987) 965 & **96**(1989) 905.

K. Mahler & J. Popken, On a maximum problem in arithmetic (Dutch), *Nieuw Arch. Wiskunde*, (3) **1**(1953) 1–15; *MR* **14**, 852e.

Daniel A. Rawsthorne, How many 1's are needed? *Fibinacci Quart.*, **27**(1989) 14–17.

F27. Mahler 对 Farey 级数的推广

n 阶 Farey 级数(Farey series)由所有分子和分母都不超过 n 的正的既约有理分数按大小顺序排列组成. 例如,5 阶 Farey 级数是

$$\frac{1}{5}\ \frac{1}{4}\ \frac{1}{3}\ \frac{2}{5}\ \frac{1}{2}\ \frac{3}{5}\ \frac{2}{3}\ \frac{3}{4}\ \frac{4}{5}\ \frac{1}{1}\ \frac{5}{4}\ \frac{4}{3}\ \frac{3}{2}\ \frac{5}{3}\ \frac{2}{1}\ \frac{5}{2}\ \frac{3}{1}\ \frac{4}{1}\ \frac{5}{1}.$$

表 10　三阶推广的 Farey 级数之片段

a	b	c	根	行列式
0	1	-1	1	
3	-1	-3	$(1+\sqrt{37})/6$	0
3	-2	-2	$(1+\sqrt{7})/3$	1
2	0	-3	$\sqrt{6}/2$	-1
3	-3	-1	$(3+\sqrt{21})/6$	1
2	-1	-2	$(1+\sqrt{17})/4$	0
1	1	-3	$(\sqrt{13}-1)/2$	-1
2	-2	-1	$(1+\sqrt{3})/2$	1
3	-2	-3	$(1+\sqrt{10})/3$	0
1	0	-2	$\sqrt{2}$	-1
3	-3	-2	$(3+\sqrt{33})/6$	1
0	2	-3	$3/2$	

由两个相邻的分数的分子和分母构成的行列式的值是 -1. Mahler 把序列中的元素看做为是系数的最大公因子为 1 且系数均不超过 n 的线性方程的正实根,由此他得到向二次方程所作的下述推广. 按照根的大小顺序列出二次方程

$$ax^2+bx+c=0, a\geqslant 0, (a,b,c)=1, b^2\geqslant 4ac,$$
$$\max\{a, |b|, |c|\}\leqslant n$$

的系数(a,b,c),此方程有正实根. 那么由任何三个相连的行中的 a,b,c 作成的三阶行列式(见 F28)似乎总是取值 0 或 ± 1. 在本书第一版中,表 10 在 $n=2$ 的情形对此作了描述,其中头一组值是$(0,1,0)$,而最后一组值是$(0,0,1)$,它们分别与根 0 和∞相对应,正如 Farey 级数可以包含项$\frac{0}{1}$和$\frac{1}{0}$一样. 我们还采用了 Selfridge 的使有理根重复的建议,以避免无意义的例外. 现在给出的表 10 是从 $n=3$ 时推广的 Farey 级数摘选来的. 表中最后一列是由该行与其相邻两行作成的行列式的值.

当 $n\leqslant 5$ 时已对猜想作了验证,但是堪培拉的 Lambertus Hesterman 对 $n=7$ 发现了反例,例如

a	b	c	根	行列式
2	-7	-7	$(7+\sqrt{105})/4$	
1	-3	-6	$(3+\sqrt{33})/2$	-2
1	-6	7	$3+\sqrt{2}$	

这是否可以加以挽救？抑或这是强小数定律的另一个例子？Lewis Low 证明了行列式的绝对值不能超过 n. 这个界是否能大大减小？

对于与三次方程有关的四阶行列式又能有什么结论呢？

参 考 文 献

H. Brown & K. Mahler, A generalization of Farey sequences: some exploration via the computer, *J. Number Theory*, **3**(1971) 364–370; *MR* **44** #3959.

Lewis Low, Some lattice point problems, PhD thesis, Univ. of Adelaide, 1979; *Bull. Austral. Math. Soc.*, **21**(1980) 303–305.

Kurt Mahler, Some suggestions for further research, Res. Report No. 20, 1983, Math. Sci. Res. Centre, Austral. Nat. Univ.

F28. 值为 1 的行列式

三阶行列式(third order determinant)

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{vmatrix}$$

可以定义为 $a_1(a_5a_9-a_6a_8)-a_2(a_4a_9-a_6a_7)+a_3(a_4a_8-a_5a_7)$.

求整数 $a_1,a_2,\cdots,a_9$,它们不取 0 或 ±1,使得

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{vmatrix} = 1 = \begin{vmatrix} a_1^2 & a_2^2 & a_3^2 \\ a_4^2 & a_5^2 & a_6^2 \\ a_7^2 & a_8^2 & a_9^2 \end{vmatrix}.$$

在第一版中我们将这问题归因于 Basil Gordon. Molnar 曾问过(他只要求 $a_i\neq\pm1$)这一问题，且不限于 3 阶行列式. 这个问题

给出一个拓扑意义，请参看 Hilton 的论著．有 Morris Newman，Peter Montgomery，Harry Applegate，Francis Coghlan 以及 Kenneth Lau 等人给出的解，其中有一些是对阶大于 3 的情形，包括若干参数解族，例如

$$\begin{vmatrix} -8n^2-8n & 2n+1 & 4n \\ -4n^2-4n & n+1 & 2n+1 \\ -4n^2-4n-1 & n & 2n-1 \end{vmatrix}.$$

Richard McIntosh 给出了有高比例的 Fibonacci 数的例子

$$\begin{vmatrix} 1167 & 2 & 5 \\ 1698 & 3 & 8 \\ 2866 & 5 & 13 \end{vmatrix} \quad \begin{vmatrix} 610 & 5 & 13 \\ 1054 & 8 & 21 \\ 1665 & 13 & 34 \end{vmatrix}.$$

Rudolf Wytek 限于考虑大于 1 的整数，在 1987 年的最后几天里用计算机找到了

$$\begin{vmatrix} 2 & 3 & 2 \\ 4 & 2 & 3 \\ 9 & 6 & 7 \end{vmatrix} \begin{vmatrix} 2 & 3 & 5 \\ 3 & 2 & 3 \\ 9 & 5 & 7 \end{vmatrix} \begin{vmatrix} 2 & 3 & 6 \\ 3 & 2 & 3 \\ 17 & 11 & 16 \end{vmatrix} \begin{vmatrix} 5 & 7 & 6 \\ 6 & 4 & 7 \\ 17 & 16 & 20 \end{vmatrix} \begin{vmatrix} 8 & 7 & 8 \\ 12 & 11 & 7 \\ 17 & 15 & 16 \end{vmatrix} \begin{vmatrix} 10 & 7 & 12 \\ 4 & 2 & 7 \\ 17 & 12 & 20 \end{vmatrix}.$$

其中第二个早先曾被 Kenneth Lau 发现过．其他的都是新的，且都不是任何参数解的特例．看起来问题的解要比一开始所想象的要多得多．

对任给的 k，当行列式的所有元素都大于或等于 k 时，Dǎnescu，Vâjâitu 和 Zaharescu 对任意阶的行列式解决了这一问题．

此问题可以推广到三次方吗？

参 考 文 献

Alexandru Dǎnescu, Viorel Vâjâitu & Alexandru Zaharescu, Unimodular matrices whose components are squares of unimodular one.

P. J. Hilton, On the Grothendieck group of compact polyhedra, *Fundamenta Math.*, **61**(1967) 199–214.

P. J. Hilton, General Cohomology Theory & K-Theory, *L.M.S. Lecture Notes*, **1**, Cambridge University Press, 1971, p. 58.

E. A. Molnar, Relation between wedge cancellation and localization for complexes with two cells, *J. Pure Appl. Alg.*, **3**(1973) 141–158.

E. A. Molnar, A matrix problem, *Amer. Math. Monthly*, **81**(1974) 383–384; and see **82**(1975) 999–1000; **84**(1977) 809 and **94**(1987) 962.
Sadao Saito, Third-order determinant: E. A. Molnar's problem, *Acta Math. Sci.*, **8**(1988) 29–34; *MR* **89j**:15031.

F29. 两个同余式，其中一个恒可解

给定一个素数 p，求一对函数 $f(x)$，$g(x)$，使得同余式 $f(x)\equiv n$，$g(x)\equiv n \bmod p$ 中有一个对所有整数 n 可解. 一个平凡的例子是 $f(x)=x^2$，$g(x)=ax^2$，其中 a 是奇素数 p 的二次非剩余(F5). Mordell 给出了进一步的例子 $f(x)=2x+dx^4$，$g(x)=x-1/4dx^2$，这里 d 是任何与 p 互素的整数，而 $1/z$ 定义为 $\bar{z}$，其中 $z\bar{z}\equiv 1 \bmod p$.

F30. 每一对取值的和均不相同的多项式

在 D1 中曾说到过尚不知道有 $a^5+b^5=c^5+d^5$ 的非平凡的解. 事实上，x^5 很可能是下述的 Erdös 的一个未解决的问题的解答：求一个多项式 $P(x)$，使所有的和 $P(a)+P(b)$ 都不相同($0\leqslant a<b$).

F31. 一个不寻常的数字问题

把整数用基数 4 来表示，即用数字 0，1，2 和 $\bar{1}(=-1)$ 来表示. 设 L 是一个整数集合，它能以这种方法用数字 0，1 和 $\bar{1}$ 表出，但是不用 2. 每个奇整数都能写成 L 中两个元素的商吗? Loxton 和 van der Poorten 证明了：给定一个奇数 k，都存在一个乘数 m，使得 m 和 km 都在 L 中，然而他们并不知道如何对最小的这样的 m 来加以估计，因而在这个意义上说，他们的分析仍然是非有效的. 或许存在一个绝对常数 C，使得总有小于 $|k|^C$ 的乘数存在. 要求大的乘数的例子有 $k=133=2011_4$，$m=333=111\bar{1}1_4$ 以及 k

$= 501 = 20\bar{1}11_4$, $m = 2739 = 1\bar{1}\ \bar{1}\ \bar{1}\ \bar{1}\ 1\bar{1}_4$.

John Selfridge 和 Carole Lacampagne 问：是否每个 $k \equiv \pm 1 \bmod 3$都可以表为两个只用到数字 1 和 $\bar{1}$(不用数字 0)表示的三进制整数之商？实验数据倾向于肯定的回答．如果允许用数字 0 和 1，但不许用数字 2，那么什么样的整数可以写成这样的商呢？

参 考 文 献

F. M. Dekking, M. Mendès France & A. J. van der Poorten, Folds! *Math. Intelligencer*, **4**(1982) 130–138, 173–181, 190–195; *MR* **84f**:10016abc.

D. H. Lehmer, K. Mahler & A. J. van der Poorten, Integers with digits 0 and 1, *Math. Comput.*, **46**(1986) 683–689; *MR* **87e**:11017.

J. H. Loxton & A. J. van der Poorten, An awful problem about integers in base four, *Acta Arith.*, **49**(1987) 193–203; *MR* **89m**:11004.

译 后 记

加拿大卡尔加里大学 R. K. 盖伊教授是一位著名数学家，他所写的《数论中未解决的问题(第二版)》是一本脍炙人口的书，书中介绍了数论中许许多多有趣的问题，它们的历史及最新发展，并且附有详尽的文献目录. 无论是对数论爱好者还是对研究数论的专家学者来说，它都是一本值得一读的好书. 本书英文版第二版出版于 1994 年，至今已有 8 年时间，因而书中的许多结果又有了新的进展. 承蒙 R. K. 盖伊将多年来世界各地读者寄给他的有关本书中问题的新进展的材料全部用电子邮件转寄给我，译者本想乘此书中文版出版之机，将所有问题的最新进展写成附录一并出版，但由于这些材料非常杂乱，数量也非常多，需要花费大量的时间加以整理、核实和编写，这决非是在短时间内可以完成的，再加上出版方面的原因，这一愿望此次未能实现. 经与科学出版社协商，除了个别必须的改动、删节外，暂定按原书英文第二版原貌出版，其他的补充材料只有待以后适当时机再行编辑出版.

在本书翻译过程中，得到原书作者 R. K. 盖伊教授的许多帮助，化解了书中的许多疑问. 在翻译过程中，译者发现了原书中数十处错误，经向作者请教都得到确认. R. K. 盖伊教授还向我指出了某些应该修改或删除的地方. 所有这些发现的错误以及应修改之处都在中文版中做了改正. 此外，还有多位数学家在本书翻译过程中对译者提出的问题给出了解答或帮助，这里应该提到的有 Samul S. Wagstaff, Gove W. Effinger, Albert Wilansky, Stephen S. T. Yau(丘成桐)和 Kevin Ford 等教授. 对上述提到的所有各位，译者谨在此表示衷心的感谢. 译者十分感谢潘承彪教授在本书翻译过程中给予的帮助. 感谢中国国家自然科学基金委员会提供的资助(NSFC 10071001). 最后，我还要特别感谢我的夫人盛筱平

女士,没有她的关心和支持,我是不可能在这么短的时间内完成这项并不轻松的任务的.

最后要提及的是,译者本想把书中提到的所有中国数学家或华人数学家的中文名字都查到,并附在他们的英文名字后面,以供读者参考. 但由于种种原因,有些人无法联系上,因而未能如愿,谨此表示我深深的歉意. 读者对本书有任何意见及建议,以及对书中涉及的问题有任何新的发现或进展,欢迎来函或来电赐教. 来信请寄:中国上海市金山区华东理工大学金山校区(邮编201512),电子邮件地址:xpsheng@jstel.net 或 mingyaozhang@yahoo.com.cn.

张明尧

2002 年 3 月 20 日

于上海市金山区辰凯花苑